VPN 3000 Series Concentrator Getting Started

Release 4.7
August 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: 78-15733
Text Part Number: 78-15733-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

VPN 3000 Series Concentrator Getting Started
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface vii

Audience vii

Organization vii

Related Documentation viii

Conventions x

Obtaining Documentation xi

Documentation Feedback xiii

Cisco Product Security Overview xiii

Obtaining Technical Assistance xiv

Obtaining Additional Publications and Information xvi

CHAPTER 1 **Understanding the VPN 3000 Concentrator** 1-1

Hardware Features 1-2

Software Features 1-4

How the VPN Concentrator Works 1-7

Where the VPN Concentrator Fits in Your Network 1-8

Physical Specifications 1-8

CHAPTER 2 **Installing and Powering Up the VPN Concentrator** 2-1

Preparing to Install 2-1

Unpacking 2-3

Installing the VPN Concentrator Hardware 2-4

Connecting Hardware 2-8

Powering Up 2-11

Beginning Quick Configuration 2-12

CHAPTER 3 **Using the VPN Concentrator Manager for Quick Configuration** 3-1

Logging in to the VPN Concentrator Manager 3-1

Starting Quick Configuration 3-3

Configuring IP Interfaces 3-4

Configuring System Information 3-8

Configuring Tunneling Protocols and Options 3-9
Configuring Address Assignment 3-10
Configuring Authentication 3-11
Configuring the Internal Server User Database 3-17
Configuring the IPSec Group 3-18
Configuring WebVPN Remote Access 3-19
Setting Up the WebVPN Home Page 3-20
Changing Admin Password 3-21
Finishing Quick Configuration 3-22
Saving the Active Configuration 3-22
What Next? 3-23
Using Other VPN Concentrator Manager Functions 3-23
Understanding the VPN Concentrator Manager Window 3-24

CHAPTER 4 **Using the Command-Line Interface for Quick Configuration** 4-1
Configuring Ethernet Interfaces 4-2
Configuring System Information 4-4
Configuring Tunneling Protocols and Options 4-5
Configuring Address Assignment 4-6
Configuring Authentication 4-8
Configuring the IPSec Group 4-14
Configuring WebVPN Remote Access 4-14
Setting Up the WebVPN Home Page 4-16
Changing the Admin Password 4-17
Completing Quick Configuration 4-17
Saving the Active Configuration 4-18
Exiting the CLI 4-18
What Next? 4-18

CHAPTER 5 **Testing the VPN Concentrator** 5-1
Before You Begin 5-1
Testing the VPN Concentrator 5-2

APPENDIX A **Troubleshooting and System Errors** A-1

Files for Troubleshooting A-1

VPN Concentrator Manager Errors A-2

Command-line Interface Errors A-5

LED Indicators A-5

APPENDIX B **Copyrights, Licenses, and Notices** B-1

Software License Agreement of Cisco Systems, Inc. B-1

Other Licenses B-4

Regulatory Standards Compliance B-10

INDEX

Preface

VPN 3000 Series Concentrator Getting Started provides information to take you from unpacking and installing the VPN 3000 Concentrator through quick configuration (configuring the minimal parameters to make it operational). You can perform quick configuration from a console with the menu-based command-line interface, or you can use the HTML-based VPN Concentrator Manager with a browser. This guide describes both methods, and we recommend the latter for ease of use.

Audience

We assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices might be new to you. You should be familiar with Windows system configuration and management, and you should be familiar with Microsoft Internet Explorer, Netscape Navigator or Communicator, or Mozilla browsers.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the VPN 3000 Concentrator	Summarizes the hardware and software features and operation. If you are familiar with VPN devices, you can skip this chapter.
Chapter 2	Installing and Powering Up the VPN Concentrator	Explains how to prepare for, unpack, install, and power up the VPN Concentrator, and how to begin quick configuration. Once you have completed the steps in this chapter, you can use *either* Chapter 3 *or* Chapter 4 to complete quick configuration.
Chapter 3	Using the VPN Concentrator Manager for Quick Configuration	Explains how to complete quick configuration of the system using the VPN Concentrator Manager with a browser. We recommend this method.
Chapter 4	Using the Command-Line Interface for Quick Configuration	Explains how to complete quick configuration of the system using the command-line interface from the console or a Telnet session.

Chapter	Title	Description
Chapter 5	Testing the VPN Concentrator	Explains how to test the system by using Microsoft Dial-Up Networking on a PC with a modem, to connect to an ISP and use PPTP to create a VPN tunnel to your private corporate network.
Appendix A	Troubleshooting and System Errors	Describes common errors that might occur while configuring or using the system, and how to correct them. It also describes all LED indicators on the VPN Concentrator and its expansion modules.
Appendix B	Appendix B, "Copyrights, Licenses, and Notices"	Specifies software agreements relevant to the VPN Concentrator.

Related Documentation

Refer to the following documents for further information about Cisco VPN applications and products.

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The short document *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator* explains how to upgrade the VPN Concentrator memory. It also explains how to upgrade the VPN Concentrator software image and bootcode to versions that support the increased memory.

The VPN Concentrator Manager also includes context-oriented online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

VPN Client Documentation

The *Cisco VPN Client User Guide for Windows,* the *Cisco VPN Client User Guide for Linux and Solaris,* and the *Cisco VPN Client User Guide for Mac OS X* explain how to install, configure, and use the VPN Client. The VPN Client lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN Concentrator.

The *VPN Client Administrator Guide* tells how to configure a VPN 3000 Concentrator for remote user connections using the VPN Client, how to automate remote user profiles, how to customize VPN Client software, how to use the VPN Client command-line interface, and how to get troubleshooting information.

VPN 3002 Hardware Client Documentation

The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.

The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is available only online.

The *VPN 3002 Hardware Client Quick Start Card* summarizes the information for quick configuration. This quick reference card is provided with the VPN 3002 and is also available online.

The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for quick configuration. It is provided with the VPN 3002 and you can also print it from the online version; you can affix the label to the VPN 3002.

Documentation on VPN Software Distribution CDs

The VPN 3000 Series Concentrator and VPN 3002 Hardware Client documentation are provided on the VPN 3000 Concentrator software distribution CD-ROM in PDF format. The VPN Client documentation is included on the VPN Client software distribution CD-ROM, also in PDF format. To view the latest versions on the Cisco web site, click the **Support** icon on the toolbar at the top of the VPN Concentrator Manager, Hardware Client Manager, or Client window. To open the documentation, you need Acrobat Reader 3.0 or later; version 4.5 is included on the Cisco VPN 3000 Concentrator software distribution CD-ROM and on the VPN Client software distribution CD-ROM.

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.
- *Virtual Private Networking: An Overview*. Microsoft Corporation: 1999. (Available from Microsoft website.)
- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following are useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, 00.10.5A.1F.4F.07).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, VPN01). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames).
Filenames	Filenames on the VPN Concentrator follow the DOS 8.3 naming convention: a maximum of eight characters for the name, plus a maximum of three characters for an extension. For example, LOG00007.TXT is a legitimate filename. The VPN Concentrator always stores filenames in uppercase.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

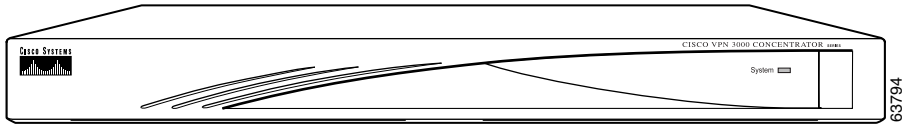
- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

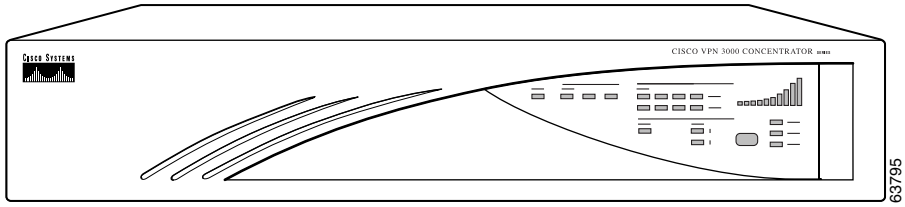
Understanding the VPN 3000 Concentrator

The VPN 3000 Concentrator (also known as the VPN Concentrator) creates a virtual private network by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. The VPN Concentrator can create single-user-to-LAN connections and LAN-to-LAN connections.

Figure 1-1 The Cisco VPN 3000 Concentrator
Model 3005



Model 3015 to 3080



Hardware Features

Current VPN Concentrator Models: 3005, 3015, 3020, 3030, 3060, and 3080.

Previous VPN Concentrator Models: C10, C20, and C50.

All systems feature:

- 10/100Base-T Ethernet interfaces (autosensing)
  - 3005: Two interfaces
  - 3015–3080: Three interfaces
- Motorola® PowerPC CPU
- SDRAM memory for normal operation
- Nonvolatile memory for critical system parameters
- Flash memory for file management

In addition, individual models have the following hardware features:

VPN Concentrator Model	Hardware Features
Model 3005	• Software-based encryption • Single power supply • 64 MB memory (versions prior to 4.1 have 32MB memory)
Model 3015	• Software-based encryption • Single power supply • Expansion capabilities: – Up to two Enhanced Cisco Scalable Encryption Processing (SEP-E) modules for hardware-based encryption – Up to two SEP-E modules for redundancy – Optional redundant power supply • 128 MB memory
Model 3020	• One SEP-E module for hardware-based encryption • Single power supply • Expansion capabilities: – Up to one additional SEP-E module for redundancy – Optional redundant power supply • 256 MB memory

VPN Concentrator Model	Hardware Features
Model 3030	• One SEP-E module for hardware-based encryption • Single power supply • Expansion capabilities: – One additional SEP-E module for hardware-based encryption – Up to two additional SEP-E modules for redundancy – Optional redundant power supply • 512 MB memory
Models 3060	• Two SEP-E modules for hardware-based encryption • Expansion capabilities: – Up to two additional SEP-E modules for system redundancy – Optional redundant power supply • 512 MB memory
Model 3080	• Two SEP-E modules for hardware-based encryption • Two SEP-E modules for system redundancy • Dual redundant power supplies • 512 MB memory

Software Features

The VPN Concentrator incorporates the following virtual private networking software features:

VPN Feature	Description
Management Interfaces	The VPN Concentrator offers multiple management interfaces. Each interface provides complete capabilities and can be used to fully configure, administer, and monitor the device. • The VPN Concentrator Manager is an HTML-based interface that lets you manage the system remotely with a standard web browser using either of the following: – HTTP connections – HTTPS (HTTP over SSL) secure connections • The VPN Concentrator command-line interface is a menu- and command-line based interface that you can use with the local system console or remotely using any of the following: – Telnet connections – SSHv1 (Secure Shell), including SCP (Secure Copy)
Tunneling Protocols	• IPSec (IP Security) Protocol – Remote access, using Cisco VPN Client or other select IPSec protocol-compliant clients – LAN-to-LAN, between peer VPN Concentrators or between a VPN Concentrator and another IPSec protocol-compliant secure gateway • L2TP over IPSec (for native Windows 2000, Windows NT, and Windows XP client compatibility) • WebVPN (clientless access using an HTTPS web browser) • PPTP (Point-to-Point Tunneling Protocol) with encryption • L2TP (Layer 2 Tunneling Protocol)
Encryption Algorithms	• 56-bit DES (Data Encryption Standard) • 168-bit Triple DES • Microsoft Encryption (MPPE): 40-bit and 128-bit RC4 • 128-bit, 192-bit, and 256-bit AES (Advanced Encryption Standard)
Authentication Algorithms	• MD5 (Message Digest 5) • SHA-1 (Secure Hash Algorithm) • HMAC (Hashed Message Authentication Coding) with MD5 • HMAC with SHA-1
Key Management	• IKE (Internet Key Exchange), formerly called ISAKMP/Oakley, with Diffie-Hellman key technique • Diffie-Hellman Group 1, Group 2, Group 5, and Group 7 (ECC) • Perfect Forward Secrecy (PFS)

VPN Feature	Description
Network Addressing Support	• DNS (Domain Name System) • Client address assignment: – DHCP (Dynamic Host Configuration Protocol), including DDNS host name population and configurable giaddr – Internally configured client IP address pools – RADIUS
Authentication and Accounting Servers	• Internal authentication server • Support for external authentication servers: – RADIUS – RADIUS with Password Expiration (MSCHAPv2) – NT Domain – Kerberos (Active Directory) – RSA Security SecurID – TACACS (administrator only) • LDAP Authorization • Authentication server testing • X.509 Digital Certificates • RADIUS accounting
Certificate Authorities	• Entrust • VeriSign • Microsoft Windows 2000 • RSA Keon • Netscape • Baltimore
Security Management	• Group and user profiles • Data traffic management, by means of: – Filters and rules (including RADIUS-based Access Control Lists) – IPSec Security Associations – NAT (Network Address Translation), many-to-one, also called PAT (Port Address Translation) – Network lists – WebVPN – Access Control List, including file shares and Web URL filtering

VPN Feature	Description
Routing Protocols	• IP • RIP v1, RIP v2 • OSPF • Static routes • Private network autodiscovery for LAN-to-LAN connections • Reverse Route Injection (RRI) allows client, LAN-to-LAN, and network extension networks to be announced via RIPv2/OSPF
Clustering	• Load Balancing • System redundancy via VRRP
System Administration	• Session monitoring and management • Software image update • Boot code upgrade • File upload • System reset and reboot • Ping • Configurable system administrator profiles • File management, including SCP and TFTP transfer • Digital certificate enrollment and management • Session limit setting • Traceroute
Monitoring	• Event logging and notification via system console, syslog, SNMP traps, and email • FTP backup of event logs • SNMP MIB-II support • System status • Session data • Memory usage • Extensive statistics

VPN Feature	Description
Client Software Compatibility	• Cisco VPN Client (IPSec): – Windows 98 and Windows ME – Windows NT® 4.0, Windows 2000, and Windows XP – Mac OS X 10.1 and 10.2 Jaguar – Linux Intel v2.2/v2.4 kernels and Solaris ULTRASparc 32-bit and 64-bit (command-line interfaces only) • Microsoft VPN Clients: – Windows® 95, Windows 98, Windows ME, Windows NT 4.0, Windows 2000, and Windows XP (PPTP) – Windows 98, Windows ME, Windows NT 4.0, Windows 2000 and Windows XP (L2TP over IPSec) • Certicom movianVPN Client (ECC, handheld)
Other Features	• Software data compression • Split tunneling • Bandwidth management

How the VPN Concentrator Works

The VPN Concentrator creates a virtual private network by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. It can create single-user-to-LAN connections and LAN-to-LAN connections.

The secure connection is called a tunnel, and the VPN Concentrator uses tunneling protocols to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. The VPN Concentrator functions as a bidirectional tunnel endpoint: it can receive plain packets, encapsulate them, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets, unencapsulate them, and send them to their final destination.

The VPN Concentrator performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel
- Manages data transfer inbound and outbound as a tunnel endpoint or router

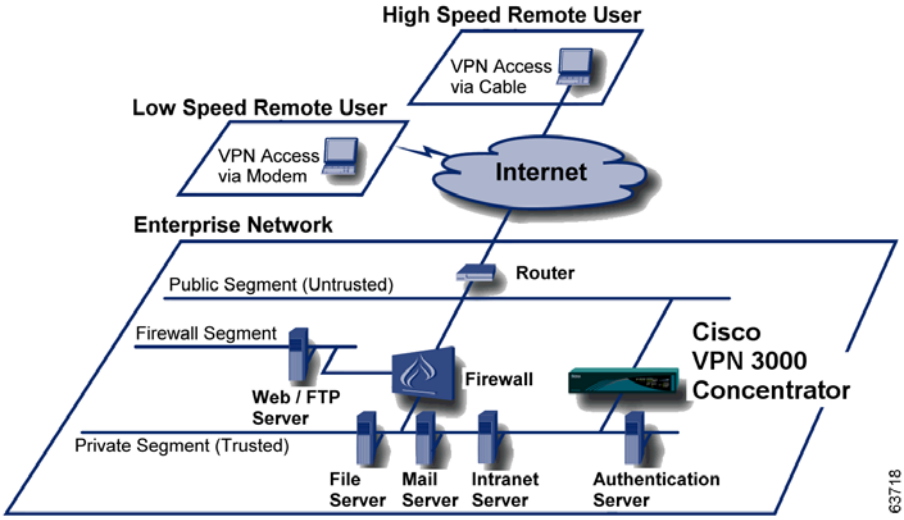
The VPN Concentrator invokes various standard protocols to accomplish these functions.

Where the VPN Concentrator Fits in Your Network

Enterprise network configurations vary widely, but the VPN Concentrator is flexible and functional enough to satisfy most applications. Figure 1-2 shows a typical installation, with the VPN Concentrator configured in parallel with a firewall, and supporting both low-speed and high-speed remote users. In some cases, the VPN Concentrator may be deployed behind the firewall; such a configuration is firewall-vendor dependent and might require additional firewall configuration.

For LAN-to-LAN or branch office applications, place a second VPN Concentrator or other IPSec protocol-compliant secure gateway at the remote office.

Figure 1-2 A Typical VPN Concentrator Network Installation



Physical Specifications

The VPN Concentrator has the following physical specifications:

Width	17.25 inches (43.8 cm); 19-inch (48.26-cm), rack mountable
Depth	• 3005 = 11.75 inches (29.85 cm) • 3015–3080 = 17 inches (43.2 cm)
Height	• 3005 = 1.75 inches (4.45 cm); 1U high form factor • 3015–3080 = 3.5 inches (8.89 cm); 2 U high form factor
Weight	• 3005 = 8.5 lbs (3.9 kg) • 3015–3080 = 27 to 33 lbs (12.25 to 15 kg), depending on model and options
Cooling	Normal operating environment, 32º to 122ºF (0º to 50ºC)

Power	100 to 240 VAC at 50/60 Hz (autosensing) • 3005 = maximum 25 W (0.2A @ 120 VAC) • 3015–3080 = maximum 50 W (0.42A @ 120 VAC)
Cabling distances from an active network device	Approx. 328 feet (100 meters)
UL approved	Electrical, mechanical, and construction
Standards compliance	FCC, E.U., and VCCI Class A compliance

CHAPTER 2

Installing and Powering Up the VPN Concentrator

This chapter tells you how to prepare for, unpack, install, and power up the VPN Concentrator, and how to begin quick configuration.

Preparing to Install

Before you begin, ensure that you have the requisite skill set and that your physical environment and software preferences are properly set, as described in the following sections.

User or Administrator Skills

We assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices may be new to you. You should be familiar with Windows system configuration and management and with Microsoft Internet Explorer, Netscape Navigator, or Mozilla browsers.

Physical Site Requirements

The VPN Concentrator requires a normal computing-equipment environment.

Power The VPN Concentrator requires only normal computing-equipment power. For maximum protection, we recommend connecting it to a conditioned power source or uninterruptible power supply (UPS). Be sure that the power source provides a reliable earth ground.

Cooling In the VPN 3005, cooling intake vents are on the front, and fans are on the rear of the chassis. In the VPN 3015–3080, cooling intake vents are on the left side, and fans on the right side, of the chassis (looking at the front). Allow at least 3 inches (75 mm) of unobstructed space on all sides. If you install the device in an equipment rack, be sure there is adequate airflow.

Access The VPN Concentrator requires access only to the front and back.

Cables and Connectors The VPN Concentrator uses the following cables and connectors:

- The VPN Concentrator Ethernet interfaces take standard UTP/STP twisted-pair network cables, Category 5, with RJ-45 8-pin modular connectors. Cisco supplies two with the system.
- The console port takes a standard straight-through RS-232 serial cable with a female DB-9 connector, which Cisco supplies with the system.

Console and PC / Telnet / Browser Requirements

The VPN Concentrator requires a console by which you enter initial configuration parameters. You can also completely configure and manage the VPN Concentrator via the CLI from the console or a Telnet client. However, for easiest use, we strongly recommend using the VPN Concentrator Manager, which is HTML-based, from a PC and browser.

The PC must be able to run the recommended browser. The console can be the same PC that runs the browser.

Browser Requirements

The VPN Concentrator Manager requires one of the following browsers:

- Microsoft Internet Explorer version 6.0 SP1 or higher (Windows) (SP2 required for Windows XP)
- Netscape Navigator version 7.2 or higher (Windows, Linux, or Solaris)
- Mozilla 1.73 or higher (Windows, Linux, or Solaris)
- Firefox 1.0 (Windows, Macintosh, or Linux)

For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

JavaScript and Cookies

Be sure JavaScript and Cookies are enabled in the browser. Check these settings.

Browser	JavaScript	Cookies
Internet Explorer 6.0	1. On the Tools menu, choose **Internet Options.** 2. On the Security tab, click **Custom Level**. 3. In the Security Settings window, scroll down to Scripting. 4. Click **Enable** under Active scripting. 5. Click **Enable** under Scripting of Java applets.	1. On the Tools menu, choose **Internet Options**. 2. On the Privacy tab, set the slider at or below **Medium High**.
Netscape Navigator 7.2 and Mozilla 1.7	1. On the Edit menu, choose **Preferences**. 2. Under the Advanced category, choose **Scripts & Plug-ins**. 3. Check the **Navigator** check box. 4. Check all **Allow Web pages** check boxes.	1. On the Edit menu, choose **Preferences**. 2. Under the Privacy & Security category, choose **Cookies**. 3. Choose **Enable All Cookies**.

Navigation Toolbar

Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh / Reload with the VPN Concentrator Manager unless instructed to do so. To protect access security, clicking Refresh / Reload automatically logs out the Manager session. Clicking Back or Forward may display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN Concentrator Manager.

Recommended PC Monitor / Display Settings

For best legibility and ease of use, we recommend setting your monitor or display as follows:

- Desktop area = 1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette = 256 colors or higher.

Unpacking

The VPN Concentrator ships with these items. Carefully unpack your device and check your contents against the list in Table 2-1. Save the packing material in case you need to repack the unit.

Table 2-1 VPN Concentrator Packing List

Check	Quantity	Item
	1	VPN 3000 Series Concentrator
	2	Rack-mounting kits—one for model 3005; one for models 3015-3080
	1	RS-232 straight-through serial console cable with DB-9 female connectors on both ends
	2	UTP network cables with RJ-45 8-pin modular connectors

Table 2-1 VPN Concentrator Packing List (continued)

Check	Quantity	Item
	1 or 2	Power cords
	1	Cisco VPN 3000 Series Concentrator CD
	1	Cisco VPN Software Client CD
	1	*VPN 3000 Series Concentrator Getting Started* (this manual)
	1	*VPN 3000 Series Concentrator Software License Agreement*
	1	*Cisco VPN Client Software License Agreement*
	1	*Export Compliance document*
	1	Cisco Product Warranty and Information packet
	1	Documentation Ordering Instructions

Installing the VPN Concentrator Hardware

You can install the VPN Concentrator in a standard 19-inch equipment rack, or just place it on a table or shelf.

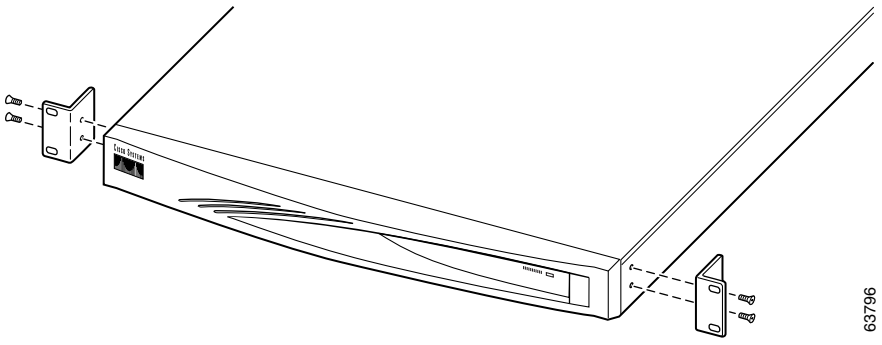
Tools Required

- No. 1 Phillips screwdriver (if you install the screw-mounted rubber feet on the device).
- No. 2 Phillips screwdriver (if you rack-mount the device).

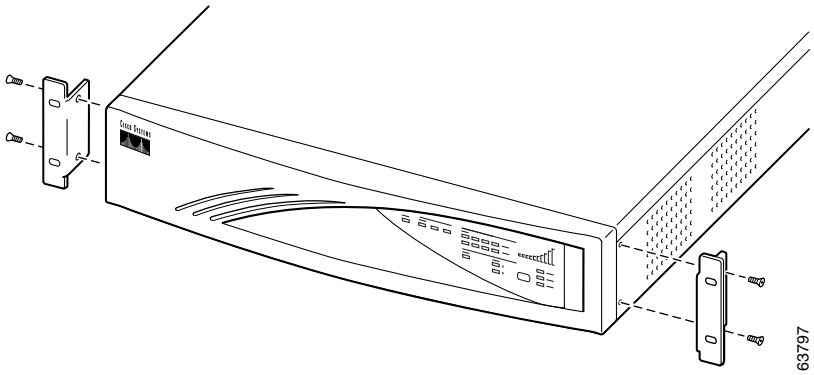
Rack Mounting

Attach the rack-mounting brackets with 10-32 screws in the holes on the front left and right sides. Be sure to orient the brackets as shown in Figure 2-1.

Figure 2-1 Attaching Rack-Mounting Brackets
Model 3005



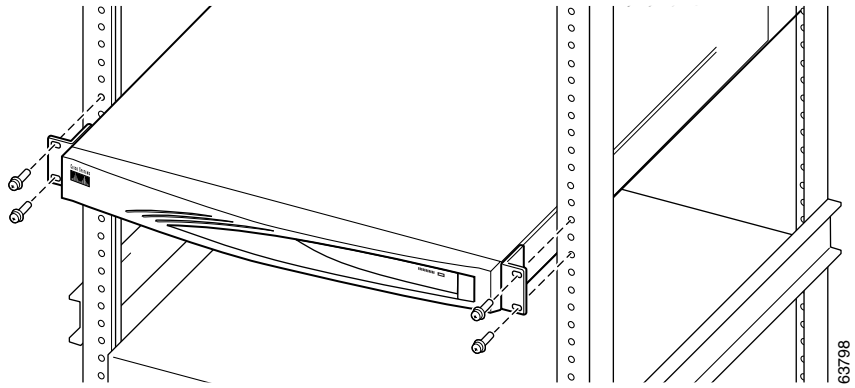
Models 3015 to 3080



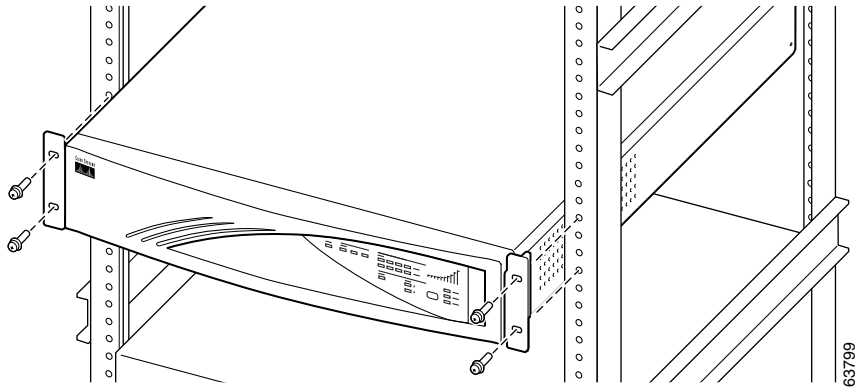
Mount the VPN Concentrator in the rack as shown in Figure 2-2. Use screws or fasteners appropriate for your equipment rack.

Figure 2-2 Rack Mounting a VPN Concentrator

Model 3005



Models 3015 through 3080



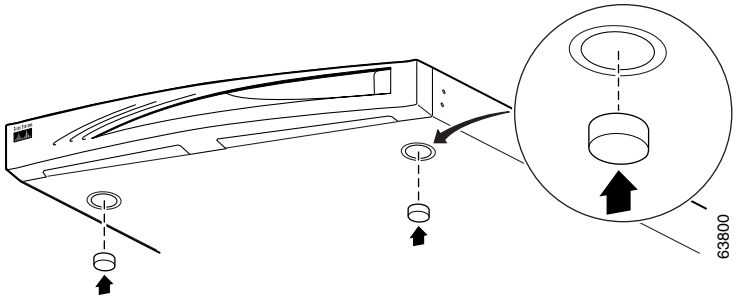
Installing Rubber Feet

To place the VPN Concentrator on a table or shelf, locate the four indentations on the bottom of the chassis. Peel the removable tape off each rubber foot, and place one foot in each indentation. (See Figure 2-3.)

Some models of the VPN Concentrator use screws to attach the rubber feet. If the rubber feet have screws, attach them to the bottom of the chassis in the holes at each corner. (See Figure 2-4.)

Figure 2-3 Installing Rubber Feet

VPN 3005



VPN 3015 - 3080

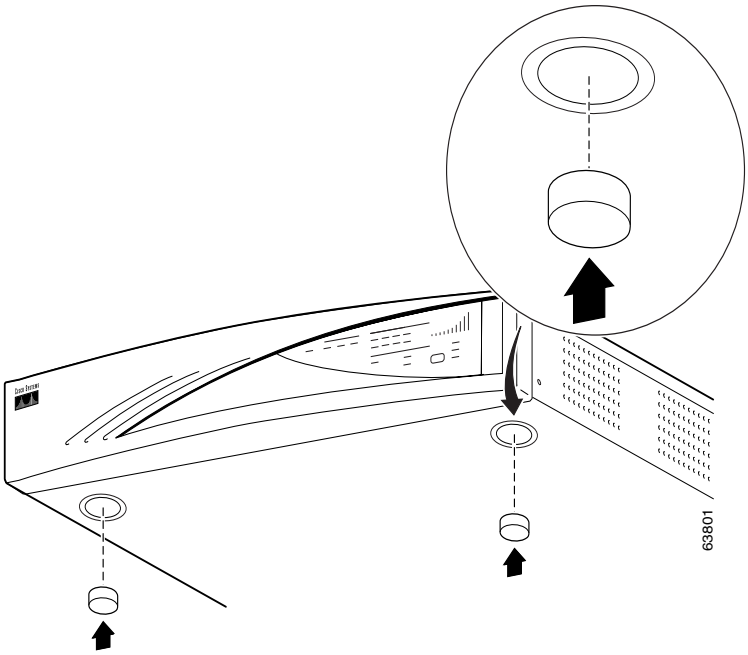
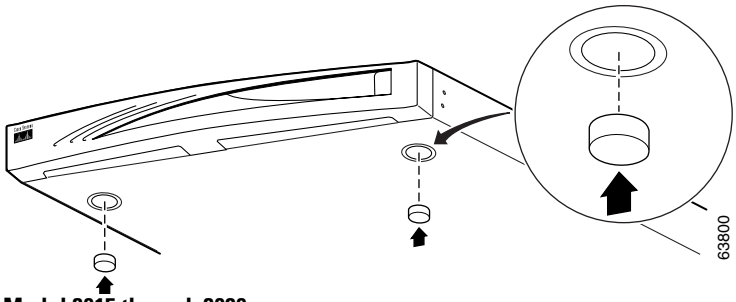
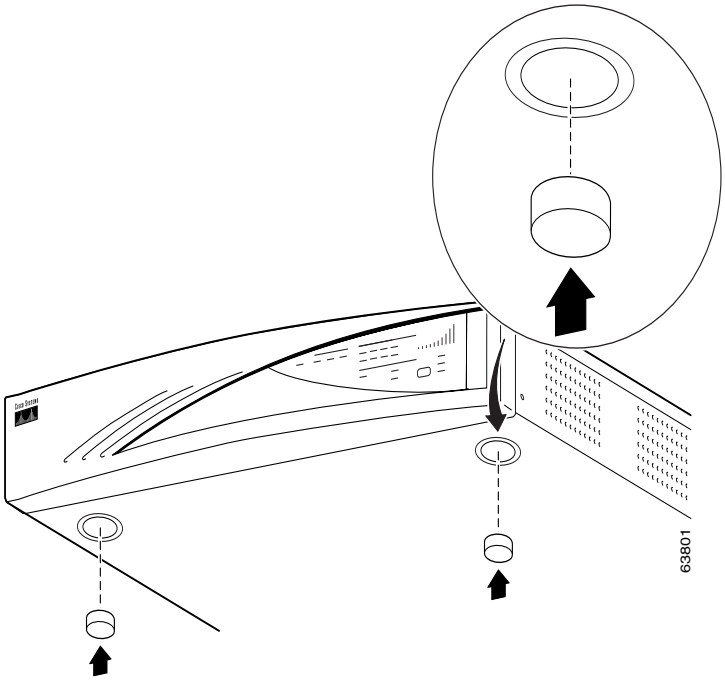


Figure 2-4 Installing Rubber Feet with Screws

Model 3005



Model 3015 through 3080



Connecting Hardware

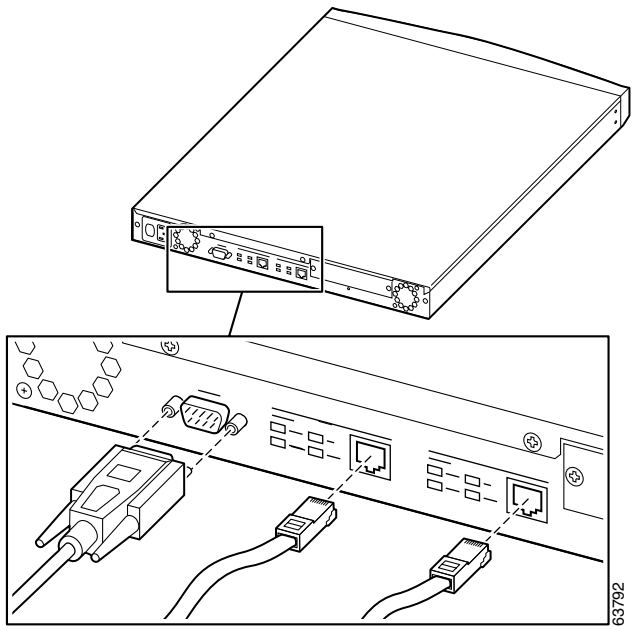
Warning **Be sure the console/PC is turned off before you connect cables to it. Do not connect power cables to the VPN Concentrator until instructed.**

Connecting the Console/PC

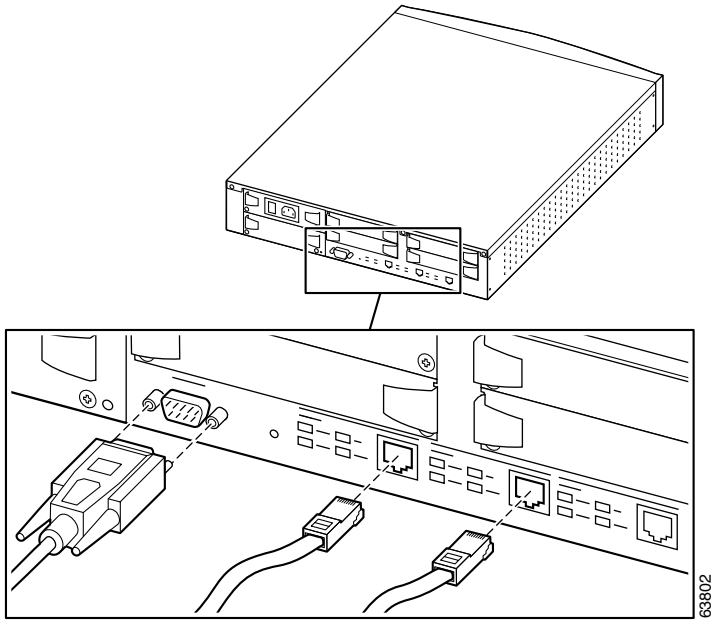
Connect the RS-232 straight-through serial cable between the Console port on the back of the VPN Concentrator and the COM1 or serial port on the console/PC. See Figure 2-5.

If you are using a PC with a browser to manage the VPN Concentrator, be sure the PC is connected to the same private LAN as the VPN Concentrator.

Figure 2-5 Connecting the Console and Network Cables
Model 3005



Model 3015 through 3080



Connecting Network Cables

Connect network patch cables between the Ethernet interface jacks on the back of the VPN Concentrator and your network patch panel or device. See Figure 2-5.

The interfaces are (left to right):

Private	Ethernet 1	VPN Concentrator interface to your private network (internal LAN)
Public	Ethernet 2	VPN Concentrator interface to the public network
External	Ethernet 3	VPN Concentrator interface to an additional LAN (present only on models 3015 – 3080)

To make the VPN Concentrator operational, you must connect at least two interfaces, usually Ethernet 1 and Ethernet 2.

Connecting Power Cable(s)

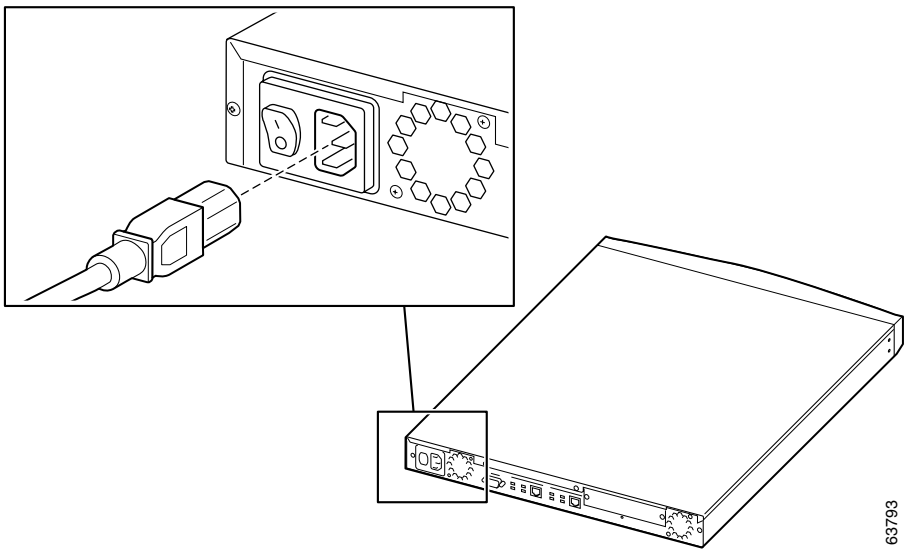
Warning **Be sure the VPN Concentrator power switch is OFF (0 depressed) before you connect a power cable. The power switch is on the power module, on the back of the VPN Concentrator.**

Connect the power cable(s) between the VPN Concentrator and an appropriate power outlet. Be sure the power outlet provides a reliable earth ground. See Figure 2-6.

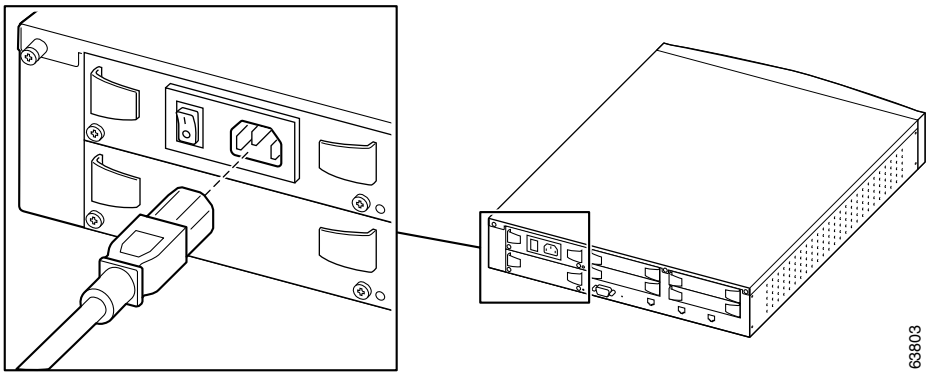
Note If you have a system with redundant power modules, make sure you connect power cables between both modules and appropriate power outlets.

Figure 2-6 Connecting Power Cable(s)

Model 3005



Model 3015 through 3080



Powering Up

Power up the devices in this sequence:

Step 1 Power up the console / PC.

Step 2 Start a terminal emulator (e.g., HyperTerminal) on the console/PC. Configure a connection to COM1, with port settings of:

- 9600 bits per second
- 8 data bits
- No parity
- 1 stop bit
- Hardware flow control.

Set the emulator for VT100 emulation, or let it auto-detect the emulation type.

Step 3 Power up the VPN Concentrator by pressing ON (**I**) on the power switch on the back. If you have a redundant system, power up both power modules.

The LED(s) on the front panel will blink and change color as the system executes diagnostics. Watch for these LEDs (if present) on the VPN Concentrator front panel to stabilize and display:

- System = green (This is the only front-panel LED on the Model 3005.)
- Ethernet Link Status 1 2 3 = green for the Ethernet interfaces to which you connected patch cables
- Expansion Modules 1 2 3 4
  - Insertion Status = green for the number of SEP-E modules in your device
    Run Status = green for the number of SEP-E modules in your device
  - Fan Status = green
- Power Supplies A B = green for the number of power supplies in your device

Ignore any other LEDs on the front panel.

Step 4 Watch for the following LEDs on the back of the device to display:

- Private / Public / External Interfaces
  Link = green for the interfaces connected to networks
- SEP-E Modules (if installed): Power = green

If LEDs that should be green are amber, red, or off, please see Appendix A, “Troubleshooting and System Errors.” Ignore any other LEDs on the back.

Step 5 The console displays initialization and boot messages such as:

```
Boot-ROM Initializing...
Boot configured 128Mb of RAM.
Image Loader Initializing...
Decompressing & loading image ............
Verifying image checksum ............
Active image loaded and verified...
Starting loaded image...
Starting power-up diagnostics...
Initializing VPN Concentrator ...
Initialization Complete...Waiting for Network...
Login: _
```

Beginning Quick Configuration

You are now ready to begin quick configuration; that is, accepting default values when possible and configuring minimal parameters to make the VPN 3000 Concentrator operational.

Note You can go through the steps of quick configuration only once, unless you reboot the system with the Reboot with Factory/Default configuration option. In that case, you can and must go through all the steps again. See Administration | System Reboot in the *VPN 3000 Concentrator Series User Guide*.

Quick configuration consists of the following steps, which are explained in the remainder of this chapter and the two chapters that follow:

Step 1 From the console, set the system time, date, and time zone.

Step 2 From the console, configure the VPN Concentrator Ethernet 1 interface to your private network.

At this point you can use a browser to complete Quick Configuration with the VPN Concentrator Manager (see Chapter 3, "Using the VPN Concentrator Manager for Quick Configuration"). While you can continue with the console instead (see Chapter 4, "Using the Command-Line Interface for Quick Configuration"), we recommend using a browser.

Step 3 Configure the other Ethernet interfaces that are connected to a public network or an additional external network.

Step 4 Enter system identification information: system name, date, time, DNS, domain name, and default gateway.

Step 5 Specify tunneling protocols and encryption options.

Step 6 Specify methods for assigning IP addresses to clients as a tunnel is established.

Step 7 Choose and identify the user authentication server: the internal server, RADIUS, NT Domain, SDI, or Kerberos/Active Directory.

Step 8 If using the internal authentication server, populate the internal user database.

Step 9 If using IPSec tunneling protocol, assign a name and password to the IPSec tunnel group.

Step 10 If using WebVPN tunneling, enable the basic WebVPN proxies for the public interface and configure the default e-mail servers.

Step 11 If using browser WebVPN, configure the WebVPN home page.

Step 12 Change the admin password for security.

Step 13 Save the configuration file. When you complete this step, quick configuration is done.

Quick Configuration Using Non-default Values

Although you can choose to accept the default values, where applicable, for many of the quick configuration parameters, you can instead specify particular values for one or more of these parameters. Table 2-2 lists the parameters you need for quick configuration and provides space for you to record the values you enter. Write those values here now to save time as you enter data.

Table 2-2 Quick Configuration Parameters

Screen | Parameter Name	Parameter Description and Use	Your Entry
IP Interfaces | Ethernet 1 (Private)	Specify the IP address and subnet mask, speed, and duplex mode for the VPN Concentrator interface to your private network.	
IP Interfaces | Ethernet 2 (Public)	Specify the IP address and subnet mask, speed, and duplex mode for the VPN Concentrator interface to the public network.	
IP Interfaces | Ethernet 3 (External)	(For models 3015–3080 only) *If so connected*, specify the IP address and subnet mask, speed, and duplex mode for the VPN Concentrator interface to an additional external network.	
System Info | System Name	Specify a device or system name for the VPN Concentrator (for example, VPN01).	
System Info | DNS Server	Specify the IP address of your local DNS (Domain Name System) server.	
System Info | Domain	Specify the registered Internet domain name to use with DNS (for example, cisco.com).	
System Info | Default Gateway	Specify the IP address or hostname of the default gateway for packets not otherwise routed.	
Tunneling	Specify the tunneling method and encryption options you want to enable.	
Address Assignment | DHCP | Server	*If you use Dynamic Host Configuration Protocol (DHCP) for remote address assignment*, specify the IP address or hostname of the DHCP server.	
Address Assignment | Configured Pool | Range Start and Range End	*If you use the VPN Concentrator to assign addresses,* specify the starting and ending IP addresses in its initial configured pool.	

Table 2-2 Quick Configuration Parameters (continued)

Screen | Parameter Name	Parameter Description and Use	Your Entry
Authentication	Your choice here determines the parameters you see in the following screen. Possible values are: • Internal Server – *Choosing* Internal Server*, means using the internal VPN Concentrator user authentication server.* On the User Database screen, specify the username and password for each user. – Additionally, *if you specify per-user address assignment*, specify the IP address and subnet mask for each user. • RADIUS *If you use an external RADIUS user authentication server*, specify its IP address or hostname, port number, and server secret or password. • NT Domain *If you use an external Windows NT Domain user authentication server,* specify its IP address, port number, and Primary Domain Controller hostname. • SDI *If you use an external SDI user authentication server,* specify its IP address and port number. • Kerberos/Active Directory *If you use an external Kerberos/Active Directory authentication server,* specify its IP address, port number, and realm.	
User Database | Group Name, Password, Verify	*If you enable the IPSec tunneling protocol,* specify a name and password for the IPSec tunnel group.	**Note** For security reasons, do not write your password here.
IPSec Group	Decide on a group name and password for the remote-access IPSec client.	
WebVPN	*If you enable WebVPN,* specify the default HTTPS, POP3S, SMTPS, or IMAP4S servers.	
WebVPN Home Page	*If you enable WebVPN using HTTPS,* configure the text and URLs that you want to appear on the WebVPN Home page.	

Using the Console

You must use the console for the first part of quick configuration—setting the system time and date, and configuring the private Ethernet interface, as described in the following steps. Then you can use the HTML-based VPN Concentrator Manager from a browser to complete quick configuration. Refer to the data you recorded in Table 2-2.

Step 1 You started the terminal emulator window on the console in the "Powering Up" section on page 2-11; if not, start it now and press **Enter** on the console keyboard until you see the login prompt. (You may see a password prompt and other messages as you press **Enter**. Ignore them and stop at the login prompt.)

```
Login: _
```

Step 2 At the cursor, enter the default login name: **admin**. At the password prompt, enter the default password: **admin**.

```
Login: admin
Password: admin
```

Step 3 The system displays the opening message and prompts you to set the time on the VPN Concentrator. The correct time is very important, so that logging and accounting entries are accurate, and so that the system can create a valid security certificate. The time in brackets is the current device time.

```
                Welcome to
              Cisco Systems
        VPN 3000 Concentrator Series
           Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.

-- : Set the time on your device. ...

> Time
Quick -> [ 15:46:41 ] _
```

At the cursor, enter the correct device time in the format HH:MM:SS, using 24-hour notation. For example, enter 4:24 p.m. as 16:24:00.

Step 4 The system prompts you to set the date. The number in brackets is the current device date.

```
-- : Enter the date ...

> Date
Quick -> [ 01/15/2005 ] _
```

At the cursor, enter the correct date in the format MM/DD/YYYY. Use four digits to enter the year. For example, enter June 16, 2005 as 06/16/2005.

Step 5 The system prompts you to set the time zone. The time zone selections are offsets relative to Greenwich Mean Time (GMT), which is the basis for Internet time synchronization. The number in brackets is the current time zone offset.

```
-- : Set the time zone on your device. ...
-- : Enter the time zone using the hour offset from GMT: ...

> Time Zone
Quick -> [ 0 ] _
```

At the cursor, enter the time zone offset in the format +/–NN. For example, enter **-5** for U.S. Eastern Standard Time.

Step 6 The system prompts you with a menu to enable DST (Daylight-Saving Time) support. During DST, clocks are set one hour ahead of standard time. Enabling DST support means that the VPN Concentrator automatically adjusts the time zone for DST or standard time. If your system is in a time zone that uses DST, you must enable DST support.

```
1) Enable Daylight Saving Time Support
2) Disable Daylight Saving Time Support

Quick -> [ 2 ] _
```

At the cursor, enter **2** to disable DST support, or enter **1** to enable DST support.

Step 7 The system prompts you to enter an IP address for Ethernet 1, which is the VPN Concentrator interface to your private network (internal LAN). Be sure no other device is using this address on your private network. *You must enter this address to continue quick configuration.*

```
This table shows current IP addresses.

    Interface             IP Address/Subnet Mask    MAC Address
-------------------------------------------------------------------
| Ethernet 1 - Private  |    0.0.0.0/0.0.0.0     |
| Ethernet 2 - Public   |    0.0.0.0/0.0.0.0     |
| Ethernet 3 - External |    0.0.0.0/0.0.0.0     |
-------------------------------------------------------------------

** An address is required for the private interface. **

> Enter IP Address
Quick Ethernet 1 -> [ 0.0.0.0 ] _
```

At the cursor, enter the IP address using dotted decimal notation; for example, 10.10.4.6.

Note Ethernet 3 appears only on Models 3015 – 3080.

Step 8 The system initializes its network subsystems, which takes a few seconds. It then prompts you for the subnet mask for the Ethernet 1 (Private) interface. The entry in brackets is the standard subnet mask for the IP address you just entered. For example, an IP address of 10.10.4.6 is a Class A address, and the standard subnet mask is 255.0.0.0.

```
> Enter Subnet Mask
Quick Ethernet 1 -> [ 255.0.0.0 ] _
```

At the cursor, enter the subnet mask appropriate for your private network addressing scheme, using dotted decimal notation; for example, 255.255.0.0. To accept the default, press **Enter**.

Step 9 The system prompts you with a menu to set the speed for the Ethernet 1 interface. You can let the VPN Concentrator automatically detect and set the appropriate speed (the default), or you can set fixed speeds of 10 or 100 Mbps (for 10BASE-T or 100BASE-T networks). If you accept the default, be sure that the port on the active network device (hub, switch, or router) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

```
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick -> [ 3 ] _
```

At the cursor, enter the menu number for your selection; for example, 1. To accept the default (3), press **Enter**.

Step 10 The system prompts you with a menu to set the transmission mode for the Ethernet 1 interface. You can let the VPN Concentrator automatically detect and set the appropriate mode (the default), or you can configure the interface for full duplex (transmission in both directions at the same time) or half duplex (transmission in only one direction at a time). If you accept the default, be sure that the port on the active network device (hub, switch, or router) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.

```
1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick -> [ 1 ] _
```

At the cursor, enter the menu number for your selection; for example, 2. To accept the default (1), press **Enter**.

Step 11 The system prompts you to enter a value for the maximum transmission unit (packet size) for this interface. Either accept the default value, 1500 bytes or specify a value in the range 68 to 1500. The standard MTU for Ethernet is 1500 bytes.

```
> MTU [68-1500)
Quick --> [1500]_
```

Step 12 The system now has enough information so that you can exit the CLI and continue configuring with a browser. The system displays one of the following menus, depending on the model of the Concentrator being configured:

Model 3005 menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> _
```

Model 3015–3080 menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Modify Ethernet 3 IP Address (External)
4) Save changes to Config file
5) Continue
6) Exit

Quick -> _
```

First, we recommend that you save your entries to the configuration file. At the cursor, enter the number for Save changes to Config file. The system redisplays the same menu.

- For easiest use, we recommend exiting and using the Manager. To do so, enter the number for Exit at the cursor and continue with the next step.
- To continue using the CLI for quick configuration, enter the number for Continue at the cursor and see Chapter 4.

Step 13 We assume you chose Exit. The system displays:

```
Done
```

Continue quick configuration with either the VPN Concentrator Manager or the command-line interface.

- To continue with the VPN Concentrator Manager, see Chapter 3, "Using the VPN Concentrator Manager for Quick Configuration."
- To continue with the command-line interface, see Chapter 4, "Using the Command-Line Interface for Quick Configuration."

Using the VPN Concentrator Manager for Quick Configuration

This chapter tells you how to complete quick configuration of the system using the VPN Concentrator Manager.

Quick configuration supplies the minimal parameters needed to make the VPN Concentrator operational, while the Main menu lets you configure all the features of the VPN 3000 Concentrator. For example, when additional parameters are configured, a configured remote user with a PC and modem can use Microsoft PPTP (point-to-point tunneling protocol) and a local ISP to connect securely—in a VPN tunnel through the Internet—with resources on a private, internal corporate network.

The VPN Concentrator Manager is an HTML-based configuration, administration, and monitoring system built into the VPN Concentrator. To use it, you need only to connect to the VPN Concentrator using a PC and browser on the same private network with the VPN Concentrator.

Before beginning the procedures in this section, you should have completed Steps 1 through 12 under Using the Console, page 2-15. As you proceed, refer to the data you recorded in the table of Table 2-2Quick Configuration Parameters, page 2-13.

The figures that follow show only the main frame of the Manager window. To use features in the other frames, see Understanding the VPN Concentrator Manager Window, page 3-24.

Note You can go through the steps of quick configuration only once, unless you reboot the system with the *Reboot ignoring the configuration file* option.

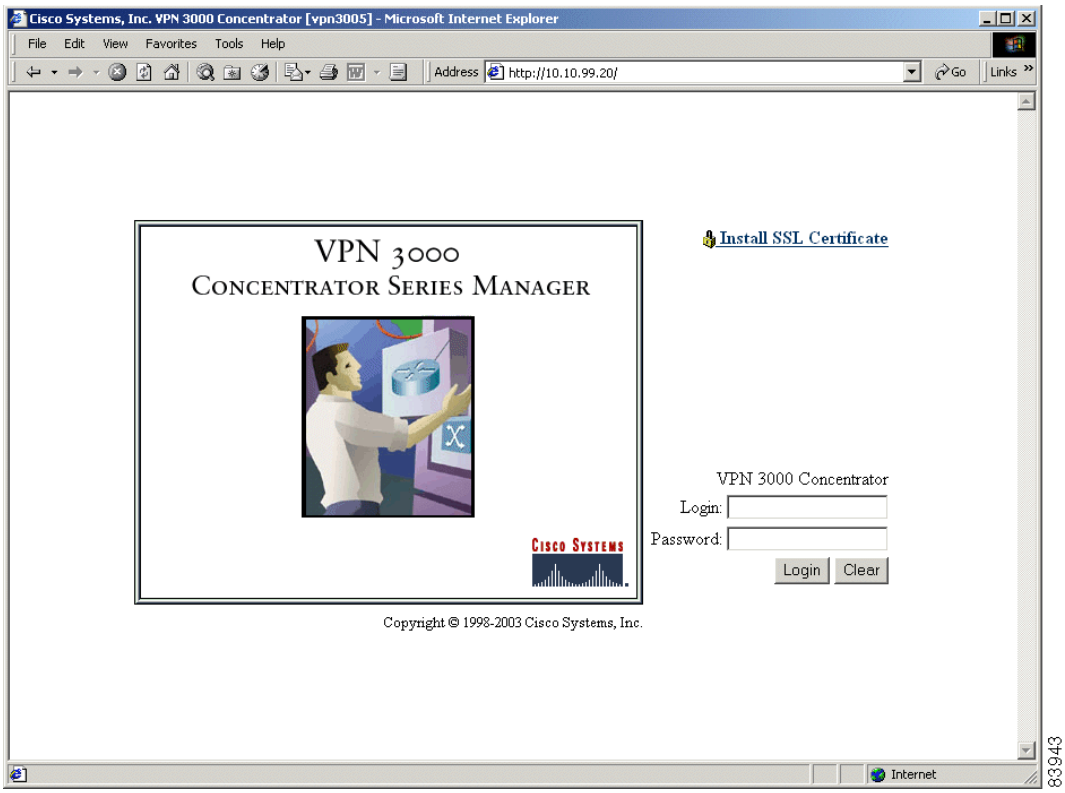
Logging in to the VPN Concentrator Manager

To access and log in to the VPN Concentrator Manager, follow these steps:

Step 1 Start the browser. See Browser Requirements, page 2-2. We recommend Microsoft Internet Explorer for best results. Maximize the browser window for easiest reading.

Step 2 With the browser, connect to the IP address of the VPN Concentrator on your private network (the address you entered in Step 7 under Using the Console, page 2-15) as an administrator. To do this, you enter <IP address>/admin (for example, 10.10.4.6/admin) in the Address or Location field. The browser displays the login screen.

Figure 3-1 VPN Concentrator Manager Login Screen



Step 3 Log in. Entries are case-sensitive, so type them exactly as shown. With Microsoft Internet Explorer, you can press the **Tab** key to move from field to field; with other browsers, you might have to change fields with the mouse. If you make a mistake, click **Clear** and start over.

a. Click in the **Login** field and type **`admin`**. (*Do not press* **Enter**.)

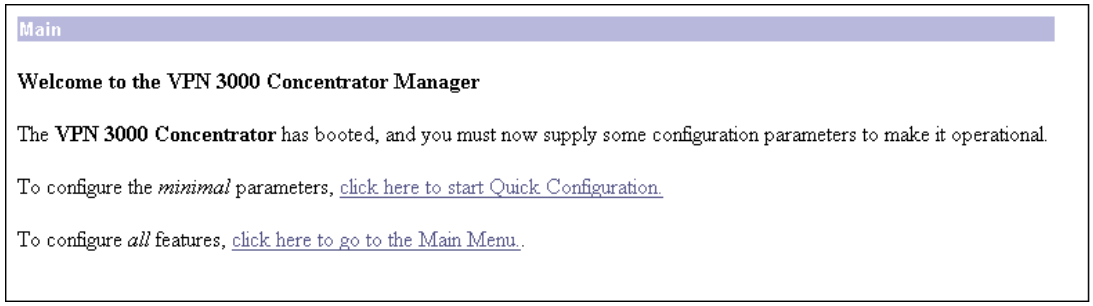
b. Click in the **Password** field and type **`admin`**. (The field shows `*****`.)

c. Click **Login**.

Starting Quick Configuration

The VPN Concentrator Manager displays the initial configuration screen (see Figure 3-1).

Figure 3-2 VPN Concentrator Manager Initial Configuration Screen


Main
Welcome to the VPN 3000 Concentrator Manager
The VPN 3000 Concentrator has booted, and you must now supply some configuration parameters to make it operational.
To configure the minimal parameters, click here to start Quick Configuration.
To configure all features, click here to go to the Main Menu.
67507

To start quick configuration, click the highlighted link that says *click here to start Quick Configuration.*

Note This screen appears only once—and you can go through the steps of quick configuration only once—unless you reboot the system with the *Reboot ignoring the configuration file* option. You cannot return to this screen if you click the highlighted link that says *click here to go to the Main Menu*.

Text entries are case-sensitive; for example, admin and ADMIN are different passwords.

After you make an entry in a field, do not press **Enter**. Just move the cursor from field to field. With Microsoft Internet Explorer, you can press **Tab** to move from field to field; other browsers may work differently.

On any screen where it appears, click **Back** to return to the previous screen.

Caution Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh / Reload with the VPN Concentrator Manager unless instructed to do so. To protect access security, clicking Refresh / Reload automatically logs out the Manager session. Clicking Back or Forward might display stale Manager screens with incorrect data or settings. To prevent mistakes while using the VPN Concentrator Manager, we recommend that you hide the browser navigation toolbar.

Configuration entries take effect as soon as you click **Apply** or **Continue**, and they constitute the active or running configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon on the Manager toolbar in the top frame of the browser window. To remind you to save your settings, the icon changes from Save to Save Needed as soon as the active configuration differs from the boot configuration.

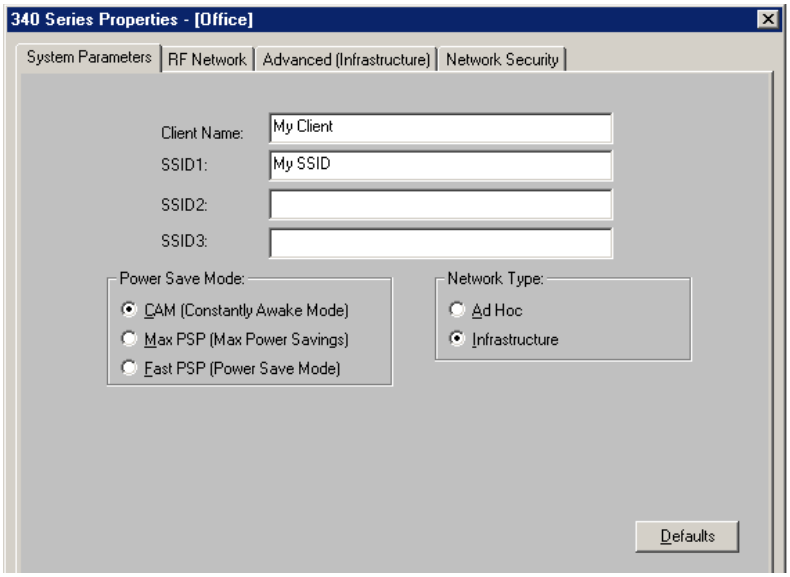
If you make a mistake and see an Error screen with the message, “An error has occurred while attempting to perform the operation,” and you return to the screen where you were working, carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost. See Appendix A, “Troubleshooting and System Errors” for more details.

Configuring IP Interfaces

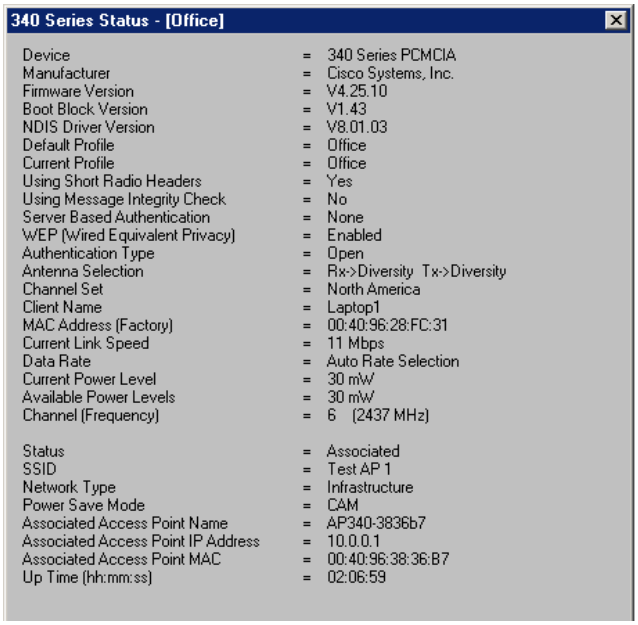
The Manager displays the Configuration | Quick | IP Interfaces screen appropriate to the model you are configuring.

Figure 3-3 Configuration | Quick | IP Interfaces Screen

Model 3005



Models 3015 through 3080


340 Series Status - [Office]
Device = 340 Series PCMCIA
Manufacturer = Cisco Systems, Inc.
Firmware Version = V4.25.10
Boot Block Version = V1.43
NDIS Driver Version = V8.01.03
Default Profile = Office
Current Profile = Office
Using Short Radio Headers = Yes
Using Message Integrity Check = No
Server Based Authentication = None
WEP (Wired Equivalent Privacy) = Enabled
Authentication Type = Open
Antenna Selection = Rx->Diversity Tx->Diversity
Channel Set = North America
Client Name = Laptop1
MAC Address (Factory) = 00:40:96:28:FC:31
Current Link Speed = 11 Mbps
Data Rate = Auto Rate Selection
Current Power Level = 30 mW
Available Power Levels = 30 mW
Channel (Frequency) = 6 (2437 MHz)
Status = Associated
SSID = Test AP 1
Network Type = Infrastructure
Power Save Mode = CAM
Associated Access Point Name = AP340-3836b7
Associated Access Point IP Address = 10.0.0.1
Associated Access Point MAC = 00:40:96:38:36:B7
Up Time (hh:mm:ss) = 02:06:59

This screen lets you configure the VPN Concentrator Ethernet interfaces.

Model 3005 comes with two Ethernet interfaces. Models 3015–3080 come with three Ethernet interfaces.

- Ethernet 1 (Private) is the interface to your private network (internal LAN).
- Ethernet 2 (Public) is the interface to the public network.
- Ethernet 3 (External), if present, is the interface to an additional LAN.

For the VPN Concentrator to become fully operational, you must configure the two interfaces you physically connected to your network under Connecting Network Cables, page 2-9.

The screen displays the current configuration settings. You entered the IP address and subnet mask for Ethernet 1 in Step 7 and Step 8 under Using the Console, page 2-15. We assume that is the interface you are using to connect to the device and configure it.

Caution If you modify any parameters of the interface that you are currently using to connect to the VPN Concentrator, you will break the connection, and you will have to restart the Manager and quick configuration from the login screen.

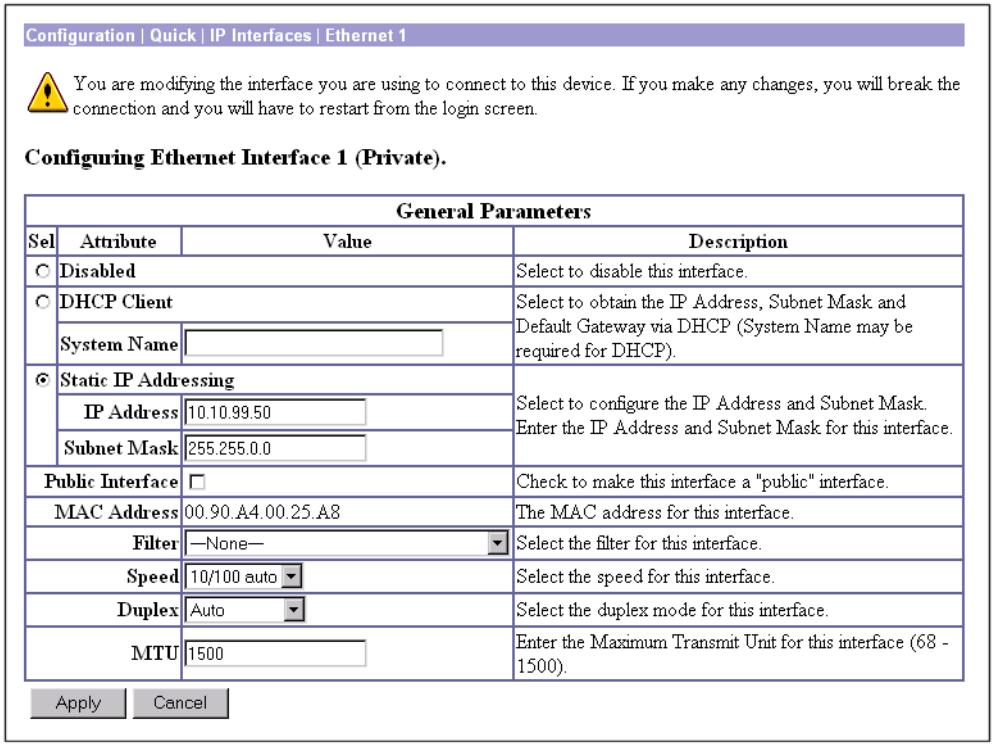
Step 1 To enter or modify parameters for an interface, click on the interface and continue, using the directions in the following section.

If you are not modifying an interface, click **Continue** to proceed, and skip to Configuring Tunneling Protocols and Options, page 3-9.

Modifying Ethernet Interface Configuration Parameters

When you click on an Ethernet interface, the Manager displays the Configuration | Quick | IP Interfaces | Ethernet screen for the interface you selected (see Figure 3-4).

Figure 3-4 Configuration | Quick | IP Interfaces | Ethernet Screen


Configuration | Quick | IP Interfaces | Ethernet 1
You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.
Configuring Ethernet Interface 1 (Private).
General Parameters
Sel
Attribute
Value
Description
Disabled
Select to disable this interface.
DHCP Client
Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP (System Name may be required for DHCP).
System Name
Static IP Addressing
Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
IP Address
10.10.99.50
Subnet Mask
255.255.0.0
Public Interface
Check to make this interface a "public" interface.
MAC Address
00.90.A4.00.25.A8
The MAC address for this interface.
Filter
—None—
Select the filter for this interface.
Speed
10/100 auto
Select the speed for this interface.
Duplex
Auto
Select the duplex mode for this interface.
MTU
1500
Enter the Maximum Transmit Unit for this interface (68 - 1500).
Apply
Cancel
78631

The screen displays the current parameters, if any, for an Ethernet interface. If you are modifying Ethernet 1, the Manager also displays a caution message. To configure parameters for an Ethernet interface, follow these steps:

Step 1 Choose one of the following options:

- If you want to disable this interface, click the **Disabled** radio button. If disabled, the interface is offline; this state lets you retain or change its configuration parameters while it is offline.
- If you want to enable this interface and use DHCP to obtain an IP address, click the **DHCP Client** radio button.
  - In the System Name field, enter a name (such as `VPN01`) for the VPN Concentrator. This name must uniquely identify this device on your network.
- If you want to enable this interface and set a static IP address for it, click the **Static IP Addressing** radio button.
  - In the IP Address field, enter the IP address for this interface, using dotted decimal notation (for example, 192.168.12.34). Be sure no other device is using this address on the network.
  - In the Subnet Mask field, enter the subnet mask for this interface, using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For instance, an IP address of 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it.

Step 2 To make this interface a public interface, check the **Public Interface** check box. A public interface is an interface to a public network, such as the Internet. You should designate only one VPN Concentrator interface as a public interface.

The MAC Address is the unique hardware MAC (Media Access Control) address for this interface, in 6-byte hexadecimal notation. The screen shows this address only after you first configure an interface, and you cannot change it.

Step 3 In the Filter field, click the drop-down menu button and select the filter that applies to this interface. The filter rules govern the handling of data packets through this interface—whether to forward or drop, according to configured criteria. You can customize filters under regular system configuration on the Configuration | Policy Management | Traffic Management screens. Cisco supplies the following default filters with the VPN Concentrator:

- 1. Private (Default)—Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)
- 2. Public (Default)—Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)
- 3. External (Default—No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)
- None—No filter applied to the interface, which means there are no restrictions on data packets.

Step 4 In the Speed field, click the drop-down menu button and select the interface speed:

- 10 Mbps—Fix the speed at 10 Mbps (10BASE-T networks)
- 100 Mbps—Fix the speed at 100 Mbps per second (100BASE-T networks)
- 10/100 auto—Let the VPN Concentrator automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). If you accept the default, be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Step 5 In the Duplex field, click the drop-down menu button and select one of the following interface transmission modes:

- Auto—Let the VPN Concentrator automatically detect and set the appropriate transmission mode, either full or half duplex (default). If you accept the default, be sure that the port on the active network device (hub, switch, or router) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.
- Full-Duplex—Fix the transmission mode as full duplex—transmission in both directions at the same time.
- Half-Duplex—Fix the transmission mode as half duplex—transmission in only one direction at a time.

Step 6 The MTU value you entered via the CLI displays in the MTU field. You do not need to edit it.

Step 7 Click **Apply** to apply your choices to the interface. Click **Cancel** to discard your choices.

The Manager returns to the Configuration | Quick | IP Interfaces screen. If you have entered new parameters for an interface, the screen displays your entries.

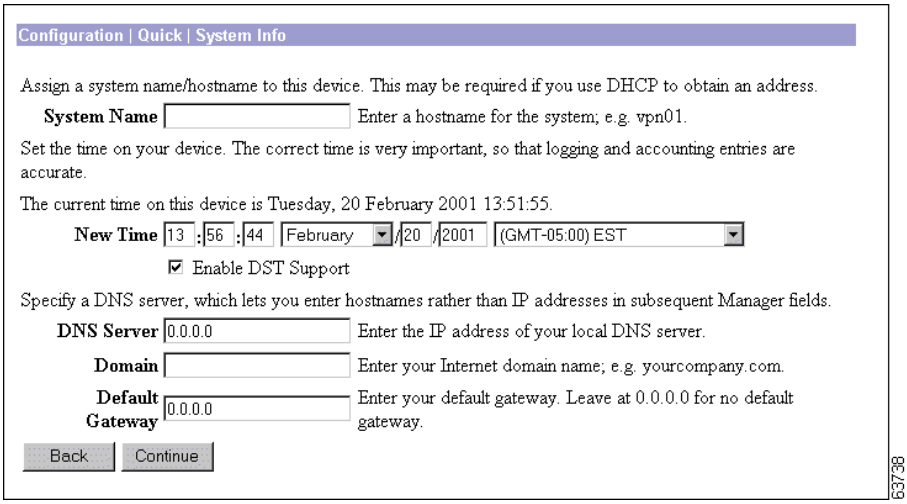
Step 8 If you want to modify another Ethernet interface, click on the interface and continue.

If you do not want to modify another interface, click **Continue** to proceed, and skip to Configuring System Information, page 3-8.

Configuring System Information

The Manager displays the Configuration | Quick | System Info screen.

Figure 3-5 Configuration | Quick | System Info Screen


Configuration | Quick | System Info
Assign a system name/hostname to this device. This may be required if you use DHCP to obtain an address.
System Name
Enter a hostname for the system; e.g. vpn01.
Set the time on your device. The correct time is very important, so that logging and accounting entries are accurate.
The current time on this device is Tuesday, 20 February 2001 13:51:55.
New Time
13 : 56 : 44
February
20 / 2001
(GMT-05:00) EST
Enable DST Support
Specify a DNS server, which lets you enter hostnames rather than IP addresses in subsequent Manager fields.
DNS Server
0.0.0.0
Enter the IP address of your local DNS server.
Domain
Enter your Internet domain name; e.g. yourcompany.com.
Default Gateway
0.0.0.0
Enter your default gateway. Leave at 0.0.0.0 for no default gateway.
Back
Continue
63738

To configure basic information that identifies your VPN Concentrator on the network, refer to the data you recorded in Table 2-2 as you follow these steps:

Step 1 The system name you entered earlier appears in the System Name field. If no system name appears, enter a name (such as `VPN01`) for the VPN Concentrator. This name must uniquely identify this device on your network.

Step 2 You previously set the time and date on the VPN Concentrator under Using the Console, page 2-15, but you can change them here if you want. The screen shows the current date and time on the device. The values shown in the New Time fields are the time on the *browser PC*, but any entries you make apply to the *VPN Concentrator*.

In the appropriate fields, make any changes. The fields are, in order: Hour : Minute : Second Month / Day / Year Time Zone. Click the drop-down menu buttons to select Month and Time Zone. The time zone selections are offsets relative to Greenwich Mean Time (GMT), which is the basis for Internet time synchronization. Enter the Year as a four-digit number.

To Enable DST Support, check the box. During DST (Daylight-Saving Time), clocks are set one hour ahead of standard time. Enabling DST support means that the VPN Concentrator automatically adjusts the time zone for DST or standard time. If your system is in a time zone that uses DST, you must enable DST support.

Step 3 In the DNS Server field, enter the IP address of your local DNS (Domain Name System) server, using dotted decimal notation (for example, 10.10.0.11).

Specifying a DNS server lets you enter Internet hostnames (for example, mail01) rather than IP addresses for servers as you configure and manage the VPN Concentrator. While hostnames are easier to remember, using IP addresses avoids problems that might arise with the DNS server offline, congested, or similarly indisposed.

Step 4 In the Domain field, enter the registered domain in which the VPN Concentrator is located (for example, cisco.com), sometimes called the domain name suffix or subdomain.

Step 5 In the Default Gateway field, enter the IP address or hostname of the system to which the VPN Concentrator should route packets that are not explicitly routed. In other words, if the VPN Concentrator has no IP routing parameters (such as RIP, OSPF, or static routes) that specify where to send packets, it will send them to this gateway. (When you first start the VPN Concentrator, it has no IP routing configuration parameters.) This address must *not* be the same as the IP address configured on any VPN Concentrator interface. To specify no default gateway, leave the field at 0.0.0.0, which means the VPN Concentrator drops unrouted packets.

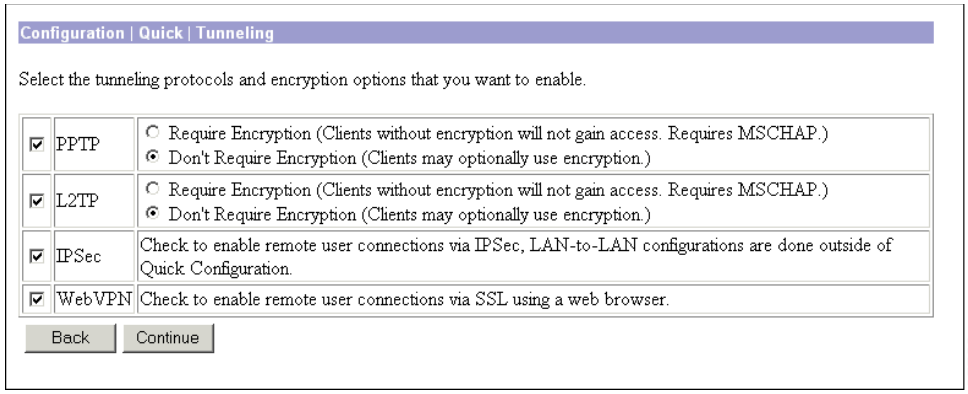
You can configure IP routing with regular system configuration. For RIP and interface-specific OSPF, see the Configuration | Interfaces screens. For global OSPF and static routes, see the Configuration | System | IP Routing screens. See the *VPN 3000 Series Concentrator Reference Volume I: Configuration* for more information.

Step 6 Click **Continue** to proceed.

Configuring Tunneling Protocols and Options

The Manager displays the Configuration | Quick | Tunneling screen.

Figure 3-6 Configuration | Quick | Tunneling Screen


Configuration | Quick | Tunneling
Select the tunneling protocols and encryption options that you want to enable.
PPTP
Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.)
Don't Require Encryption (Clients may optionally use encryption.)
L2TP
Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.)
Don't Require Encryption (Clients may optionally use encryption.)
IPSec
Check to enable remote user connections via IPSec, LAN-to-LAN configurations are done outside of Quick Configuration.
WebVPN
Check to enable remote user connections via SSL using a web browser.
Back
Continue
97738

You must enable at least one of these protocols for the device to function as a VPN device. PPTP and L2TP are popular with Microsoft Windows-based clients, and the VPN 3000 Client uses IPSec. WebVPN provides remote access over the Internet, and does not require either a software or hardware client. To enable, disable, and configure virtual private network tunneling protocols and encryption options on the VPN Concentrator, follow these steps:

Step 1 Check **PPTP** to enable Point-to-Point Tunneling Protocol. (This box is checked by default.)

Step 2 *If you enable PPTP*, click one of the radio buttons to select the encryption option:

- Require Encryption—PPTP connections must use Microsoft encryption to encrypt data. This option requires MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) and provides maximum security. During connection setup, clients must agree to use encryption or they will not be connected.

- Don't Require Encryption—PPTP connections may use Microsoft encryption to encrypt data (the default). During connection setup, clients may or may not agree to use Microsoft encryption; they will be connected in either case.

Step 3 Check **L2TP** to enable Layer 2 Tunneling Protocol. (This box is checked by default.)

Step 4 *If you enable L2TP*, click one of the radio buttons to select the encryption option:

- Require Encryption—L2TP connections must use Microsoft encryption to encrypt data. This option requires MS-CHAP and provides maximum security. During connection setup, clients must agree to use encryption or they will not be connected.
- Don't Require Encryption—L2TP connections may use Microsoft encryption to encrypt data (the default). During connection setup, clients may or may not agree to use Microsoft encryption; they will be connected in either case.

Step 5 Check **IPSec** to enable remote-access user connections using Internet Protocol Security protocol. (This box is checked by default.) This option supports only remote-access IPSec connections from the VPN 3000 Client or a similar protocol-compliant client. To configure IPSec LAN-to-LAN connections, see Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN under regular system configuration.

Step 6 Check **WebVPN** to enable remote-access user connections via SSL using a web browser or e-mail client.

Step 7 Click **Continue** to proceed.

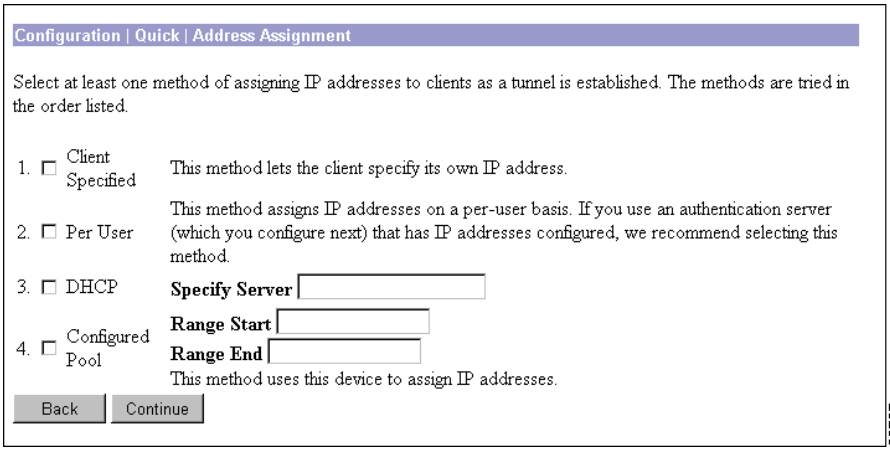
If you enable *none* of the protocols, skip to the section on Changing Admin Password, page 3-21.

If you enable *at least one* protocol, continue to the next section.

Configuring Address Assignment

The Manager displays the Configuration | Quick | Address Assignment screen. This screen appears only when you enable at least one tunneling protocol.

Figure 3-7 Configuration | Quick | Address Assignment Screen


Configuration | Quick | Address Assignment
Select at least one method of assigning IP addresses to clients as a tunnel is established. The methods are tried in the order listed.
1. Client Specified
This method lets the client specify its own IP address.
2. Per User
This method assigns IP addresses on a per-user basis. If you use an authentication server (which you configure next) that has IP addresses configured, we recommend selecting this method.
3. DHCP
Specify Server
4. Configured Pool
Range Start
Range End
This method uses this device to assign IP addresses.
Back
Continue
63727

Here you select the methods for assigning IP addresses to clients during tunnel establishment. The VPN Concentrator tries these methods in the order listed.

To select a method, follow these steps.

Step 1 Check **Client Specified** to enable this method, which lets the client specify its own IP address. If you use IPSec, you must check additional boxes, since IPSec does not allow client-specified IP addresses.

Step 2 Check **Per User** to enable this method, which assigns IP addresses on a per-user basis. If you use an authentication server that has IP addresses configured, we recommend using this method. You configure an authentication server on the next screen.

Step 3 Check **DHCP** (Dynamic Host Configuration Protocol) to enable this method, which uses a DHCP server to assign IP addresses.

Step 4 *If you enable DHCP*, enter the DHCP server hostname or IP address in the Specify Server field. (If you configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Step 5 Check **Configured Pool** to enable this method, which uses the VPN Concentrator to assign IP addresses from an internally configured pool.

Step 6 *If you enable Configured Pool*, enter the starting and ending IP addresses available in the initial pool, in the Range Start and Range End fields. Enter these addresses in dotted decimal notation; for example, 10.10.147.77.

Step 7 Click **Continue** to proceed.

When you configure the VPN Concentrator to service IPSec or L2TP VPN clients, you must configure the users, users' Group, or Base Group to allocate client VPN (private side) addresses. VPN clients (as opposed to Clientless access) require that the VPN Concentrator provide private-side IP addresses which the clients then use to configure their virtual network adaptors.

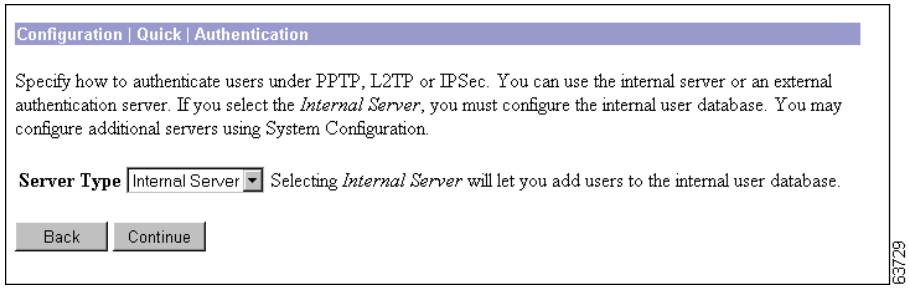
You can configure these settings in the regular VPN Concentrator Manager on the following screens:

- **Configuration | System | Address Management** — Set up a source of client addresses for Base Group configuration and inherited groups.
- **Configuration | User Management | Groups | Address Pools** — Set up address pools for specific user groups.
- **Configuration | User Management | Users | Modify** — Configure specific addresses for particular users.

Configuring Authentication

The Manager displays the Configuration | Quick | Authentication screen. This screen appears only when you enable at least one tunneling protocol.

Figure 3-8 Configuration | Quick | Authentication Screen, Internal Server


Configuration | Quick | Authentication
Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the Internal Server, you must configure the internal user database. You may configure additional servers using System Configuration.
Server Type
Internal Server
Selecting Internal Server will let you add users to the internal user database.
Back
Continue
63729

You can choose how to authenticate users. You can select the VPN Concentrator internal server or one of three external server types. You must select one server type. You can configure additional authentication servers on the Configuration | System | Servers | Authentication screen using regular system configuration.

Click the drop-down menu button and select the Server Type. The screen and its configurable fields change depending on the Server Type. Choose one of the following:

- Internal Server—The internal VPN Concentrator authentication server. (This is the default selection.)
- RADIUS—An external Remote Authentication Dial-In User Service server.
- NT Domain—An external Windows NT Domain server.
- SDI—An external RSA Security Inc. SecurID server.
- Kerberos/Active Directory—An external Windows/Active Directory server or a UNIX/Linux Kerberos server.

Before you configure an external server here, be sure that the external server you reference is itself properly configured and that you know how to access it (IP address or hostname, TCP/UDP port, secret/password, and so forth). The VPN Concentrator functions as the client of these servers.

Find your selected Server Type in the following sections and follow the configuration instructions there.

Internal Server Type

The VPN Concentrator internal authentication server lets you enter a maximum of 100 groups and users (combined) in its database, which is adequate for a small user base. For larger numbers of users, we recommend using an external authentication server. See the Configuration | User Management screens under regular System Configuration.

The internal server has no configurable parameters.

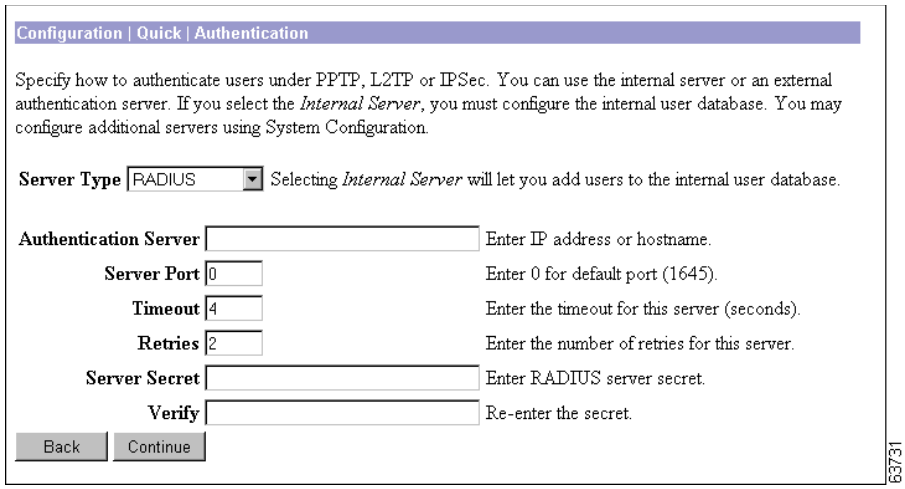
Click **Continue** to proceed.

Skip to the section Configuring the Internal Server User Database, page 3-17.

RADIUS Server Type

External RADIUS servers can return group and user authentication parameters that match those on the VPN Concentrator; other authentication servers do not. The VPN 3000 software CD-ROM includes a link that customers with Cisco.com logins can use to access an evaluation copy of the CiscoSecure ACS RADIUS authentication server. The VPN 3000 software CD-ROM also has current VPN 3000 VSA registry files that let customers load new supported attributes on their ACS server, and provides instructions for using them.

Figure 3-9 Configuration | Quick | Authentication Screen, RADIUS Server


Configuration | Quick | Authentication
Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the Internal Server, you must configure the internal user database. You may configure additional servers using System Configuration.
Server Type RADIUS Selecting Internal Server will let you add users to the internal user database.
Authentication Server Enter IP address or hostname.
Server Port 0 Enter 0 for default port (1645).
Timeout 4 Enter the timeout for this server (seconds).
Retries 2 Enter the number of retries for this server.
Server Secret Enter RADIUS server secret.
Verify Re-enter the secret.
Back
Continue
63731

We suggest you accept the default values where available. To configure these parameters for a RADIUS (Remote Authentication Dial-In User Service) authentication server, follow these steps:

Step 1 In the Authentication Server field, enter the hostname or IP address of the external RADIUS server. If you configured a DNS server, you can enter a hostname (maximum 32 characters); otherwise, enter an IP address.

Step 2 In the Server Port field, enter the UDP port number by which you access the server. Enter `0` to have the system supply the default port number, 1645.

Step 3 In the Timeout field, enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. Minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Step 4 In the Retries field, enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative. Minimum is 0, default is 2, maximum is 10 retries.

Step 5 In the Server Secret field, enter the RADIUS server secret (also called the shared secret); for example, C8z077f. The maximum is 64 characters. The field shows only asterisks.

Step 6 In the Verify field, re-enter the RADIUS server secret to verify it. The field shows only asterisks.

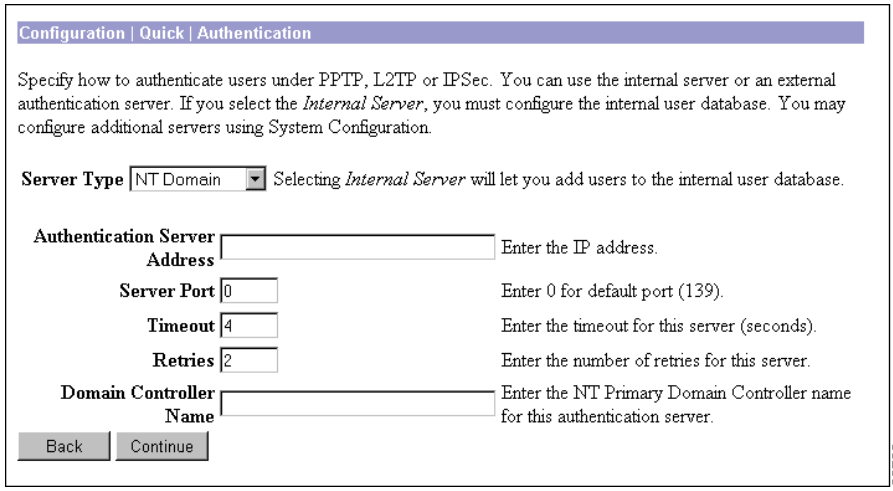
Step 7 Click **Continue** to proceed.

If you selected the IPSec tunneling protocol, skip to the section Configuring the IPSec Group, page 3-18. Otherwise, skip to the section Changing Admin Password, page 3-21.

NT Domain Server Type

Configure these parameters for an external Windows NT Domain authentication server. We suggest you accept the default values. (See Figure 3-10.)

Figure 3-10 Configuration | Quick | Authentication Screen, NT Domain Server


Configuration | Quick | Authentication
Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the Internal Server, you must configure the internal user database. You may configure additional servers using System Configuration.
Server Type
NT Domain
Selecting Internal Server will let you add users to the internal user database.
Authentication Server Address
Enter the IP address.
Server Port
0
Enter 0 for default port (139).
Timeout
4
Enter the timeout for this server (seconds).
Retries
2
Enter the number of retries for this server.
Domain Controller Name
Enter the NT Primary Domain Controller name for this authentication server.
Back
Continue
63730

To configure the parameters for the NT authentication server, follow these steps:

Step 1 In the Authentication Server Address field, enter the IP address of the NT Domain authentication server; for example, 192.168.12.34. Use dotted decimal notation.

Step 2 In the Server Port field, enter the TCP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 139.

Step 3 In the Timeout field, enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Step 4 In the Retries field, enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative. The minimum is 0, default is 2, maximum is 10 retries.

Step 5 In the Domain Controller Name field, enter the NT Primary Domain Controller hostname for this server; for example, PDC01.The maximum is 16 characters. You must enter this name, and it must be the correct hostname for the server whose IP address you entered in Authentication Server Address above; if it is incorrect, authentication will fail.

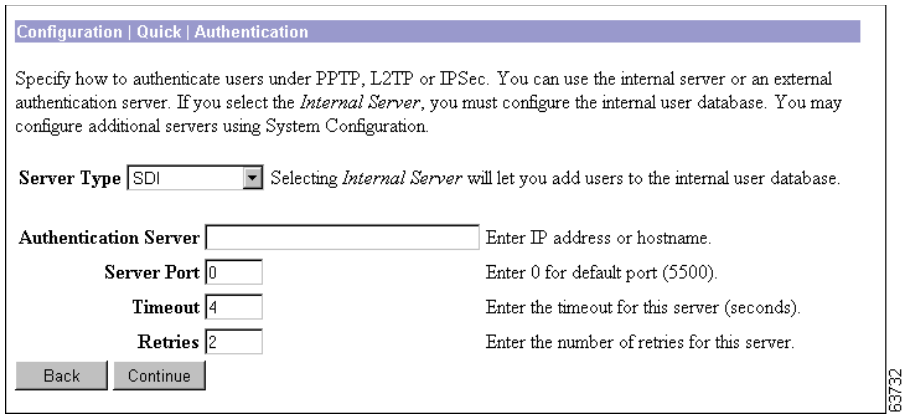
Step 6 Click **Continue** to proceed.

If you selected the IPSec tunneling protocol, skip to the section Configuring the IPSec Group, page 3-18. Otherwise, skip to the section Changing Admin Password, page 3-21.

SDI Server Type

Configure these parameters for an external SDI (RSA Security Inc. SecurID) authentication server. We suggest you accept the defaults.

Figure 3-11 Configuration | Quick | Authentication Screen, SDI Server


Configuration | Quick | Authentication
Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the Internal Server, you must configure the internal user database. You may configure additional servers using System Configuration.
Server Type
SDI
Selecting Internal Server will let you add users to the internal user database.
Authentication Server
Enter IP address or hostname.
Server Port
0
Enter 0 for default port (5500).
Timeout
4
Enter the timeout for this server (seconds).
Retries
2
Enter the number of retries for this server.
Back
Continue
63732

To configure the parameters for the SDI authentication server, follow these steps:

Step 1 In the Authentication Server field, enter the hostname or IP address of the external SDI server. The maximum is 32 characters. (If you configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Step 2 In the Server Port field, enter the UDP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 5500.

Step 3 In the Timeout field, enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Step 4 In the Retries field, enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative. The minimum is 0, default is 2, maximum is 10 retries.

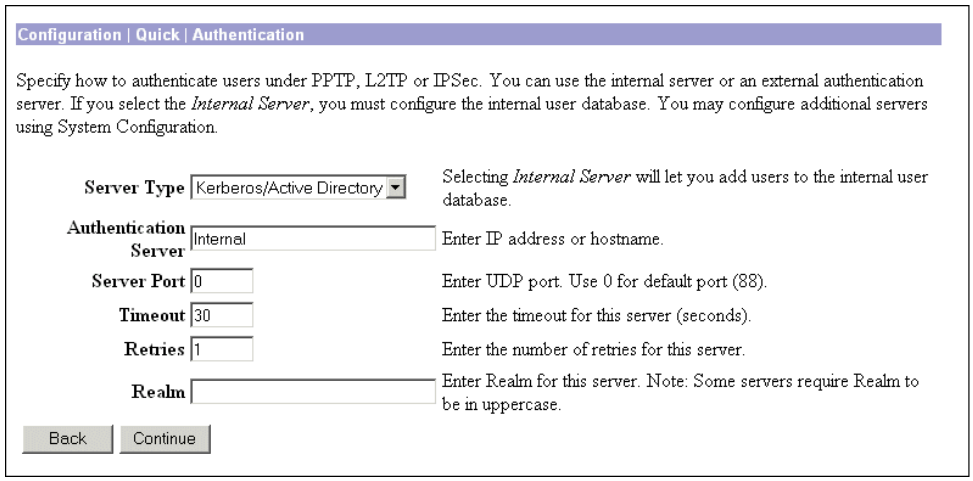
Step 5 Click **Continue** to proceed.

If you selected the IPSec tunneling protocol, skip to the section Configuring the IPSec Group, page 3-18. Otherwise, skip to the section Changing Admin Password, page 3-21.

Kerberos/Active Directory Server Type

Configure these parameters for an external Windows/Active Directory server or a UNIX/Lynx Kerberos server.

Figure 3-12 Configuration | Quick | Authentication Screen, Kerberos/Active Directory Server


Configuration | Quick | Authentication
Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the Internal Server, you must configure the internal user database. You may configure additional servers using System Configuration.
Server Type
Kerberos/Active Directory
Selecting Internal Server will let you add users to the internal user database.
Authentication Server
Internal
Enter IP address or hostname.
Server Port
0
Enter UDP port. Use 0 for default port (88).
Timeout
30
Enter the timeout for this server (seconds).
Retries
1
Enter the number of retries for this server.
Realm
Enter Realm for this server. Note: Some servers require Realm to be in uppercase.
Back
Continue
104078

To configure the parameters for the Kerberos/Active Directory server, follow these steps:

Step 1 In the Authentication Server field, enter the hostname or IP address of the external Kerberos/Active Directory authentication server.

Step 2 In the Server Port field, enter the TCP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 88.

Step 3 In the Timeout field, enter the time in seconds to wait, after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default time is 4 seconds. The maximum time is 30 seconds.

Step 4 In the Retries field, enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next Kerberos/Active Directory authentication server in the list. The minimum number of retries is 0. The default number of retries is 2. The maximum number of retries is 10.

Step 5 In the Realm field, enter the realm name for this server, for example: USDOMAIN.ACME.COM. You must enter this name, and it must be the correct realm name for the server for which you entered the IP address in Authentication Server. If it is incorrect, authentication will fail.

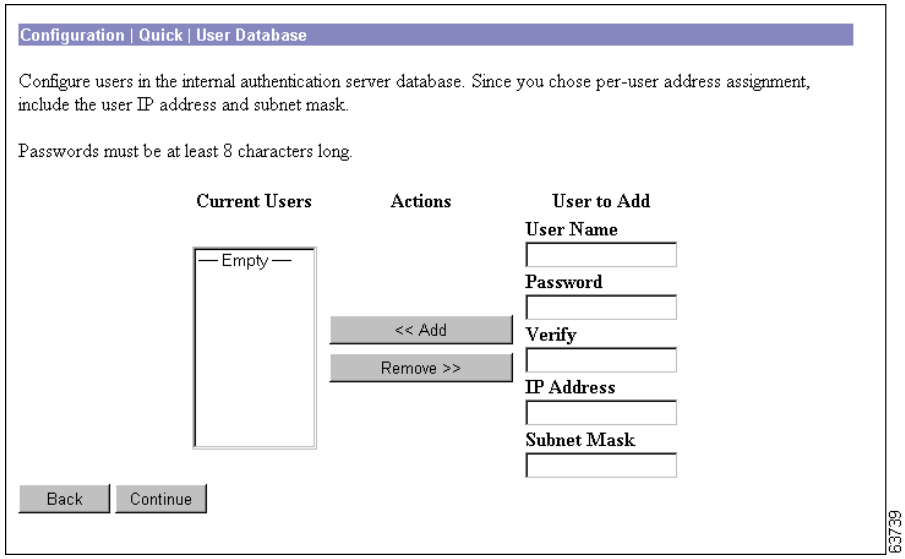
The following types of servers require that you enter the realm name in all uppercase letters: Windows 2000, Windows XP, and Windows .NET. For these types of servers, if the letters are not uppercase, authentication will fail.

If you selected the IPSec tunneling protocol, skip to the section Configuring the IPSec Group, page 3-18. Otherwise, skip to the section Changing Admin Password, page 3-21.

Configuring the Internal Server User Database

The Manager displays the Configuration | Quick | User Database screen. This screen displays only when you select the internal authentication server.

Figure 3-13 Configuration | Quick | User Database Screen



This screen lets you add and remove users in the internal authentication server database. When you first do quick configuration, the Current Users list is empty. To use the internal server, you must add at least one user to the database. As you add or remove users, the system updates and refreshes the screen with the appropriate entries in the Current Users list.

You can change user parameters on the regular Configuration | User Management | Users screens, but on this quick configuration screen, you can only add and remove users. Follow these steps to add or remove a user:

Step 1 Under User to Add:

a. Type a unique name in the User Name field. Maximum is 32 characters, case-sensitive. To be authenticated, the user must log in from the client using this name.

b. Move to the Password field and type the password. The password must be at least 8 characters long; maximum is 32 characters, case-sensitive. The field shows only asterisks. To be authenticated, the user must log in from the client using this password. Each user name / password combination must be unique.

c. Move to the Verify field and retype the password. The field shows only asterisks.

d. *If you selected per-user address assignment:*

- Move to the IP Address field and enter the user IP address in dotted decimal notation; for example, 10.10.1.35. This is the IP address assigned to this user as a client. This field is not present if you selected other address assignment methods.
- Move to the Subnet Mask field and enter the user subnet mask in dotted decimal notation; for example, 255.255.0.0. This is the subnet mask assigned to this user as a client. This field is not present if you selected other address assignment methods.

Step 2 Click **<< Add**.

Step 3 Repeat Steps 1 and 2 for each user. The screen refreshes each time you add a user.

Step 4 To remove a user, select the user in the Current Users list and click **Remove >>**. The screen refreshes each time you remove a user. *There is no confirmation or undo*; to reinstate a user, enter the data in Step 1.

Step 5 When you have finished entering users, click **Continue** to proceed.

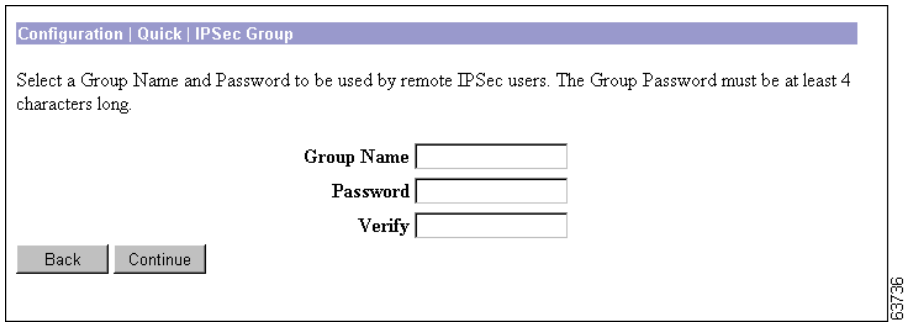
If you selected the IPSec tunneling protocol, proceed to the section "Configuring the IPSec Group" below. Otherwise, skip to the section Changing Admin Password, page 3-21.

Configuring the IPSec Group

The Manager displays the Configuration | Quick | IPSec Group screen. This screen appears only when you select the IPSec tunneling protocol, and you must configure these parameters to complete quick configuration.

The remote-access IPSec client connects to the VPN Concentrator using this group name and password, which are automatically configured on the internal authentication server. This is the IPSec group that creates the tunnel. Users then log in, and are authenticated, through their usernames and passwords. (See Figure 3-14.)

Figure 3-14 Configuration | Quick | IPSec Group Screen


Configuration | Quick | IPSec Group
Select a Group Name and Password to be used by remote IPSec users. The Group Password must be at least 4 characters long.
Group Name
Password
Verify
Back
Continue
63736

Step 1 In the Group Name field, enter a unique name for this group. The maximum field length is 32 characters. Entries are case-sensitive.

Step 2 In the Password field, enter a unique password for this group. The minimum field length is 4 characters. The maximum length is 32 characters. Entries are case-sensitive. The field displays only asterisks.

Step 3 In the Verify field, reenter the group password to verify it. The field displays only asterisks.

Step 4 Click **Continue** to proceed. You must configure these parameters before you can proceed.

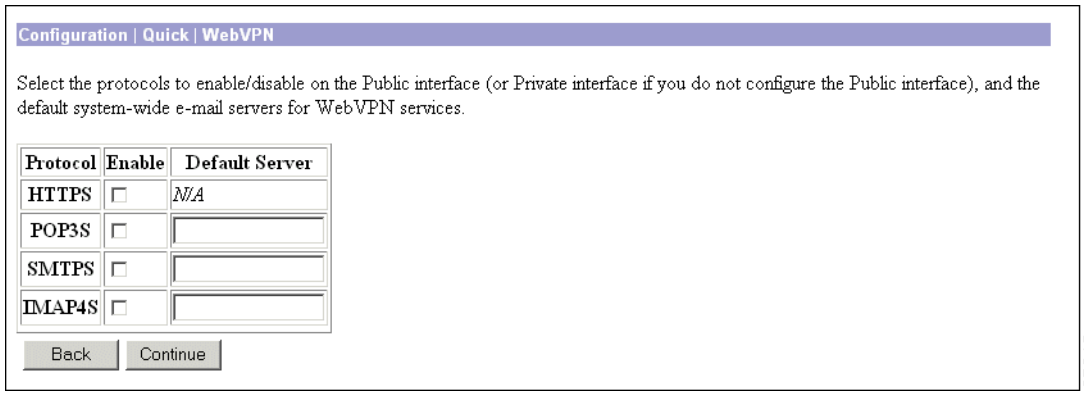
Configuring WebVPN Remote Access

The Manager displays the WebVPN Remote Access screen. WebVPN allows remote users to access the corporate network from any computer with an Internet connection to use e-mail, files, or internal websites. This screen allows you to:

- Enable WebVPN (HTTPS) connections
- Enable and configure POP3S, IMAP4S, and SMTPS sessions to use e-mail proxy.

This screen appears only if you enabled WebVPN on the Configuration | Quick | Tunneling screen.

Figure 3-15 Configuration | Quick | WebVPN Screen



Step 1 To enable WebVPN connections to the public interface of the VPN Concentrator, check the HTTPS **Enable** check box. If you have not configured the Public Interface, WebVPN connections are enabled on the Private interface instead.

Step 2 To enable POP3S, IMAP4S, or SMTPS sessions to use e-mail proxy, check the corresponding Enable check box, and enter the IP address or host name of the default mail server.

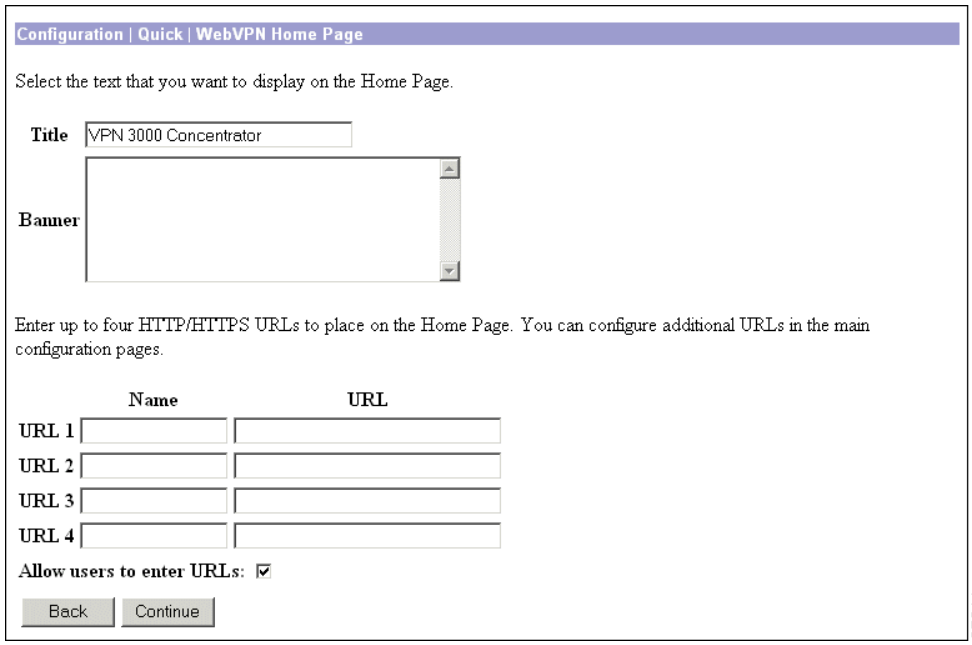
Step 3 Click **Continue**.

Setting Up the WebVPN Home Page

The Manager displays the WebVPN Home Page screen. This screen allows you to customize the home page that WebVPN users will see when they log in. In this screen you can change the title, add a banner, and configure up to four URLs.

This screen appears only if you enabled WebVPN on the Configuration | Quick | Tunneling screen.

Figure 3-16 Configuration | Quick | WebVPN Home Page


Configuration | Quick | WebVPN Home Page
Select the text that you want to display on the Home Page.
Title
VPN 3000 Concentrator
Banner
Enter up to four HTTP/HTTPS URLs to place on the Home Page. You can configure additional URLs in the main configuration pages.
Name
URL
URL 1
URL 2
URL 3
URL 4
Allow users to enter URLs:
Back
Continue
97944

Step 1 Enter the title to appear on each WebVPN page.

Step 2 Enter a banner to appear on the WebVPN home page.

Step 3 You can set up links to websites to appear on the WebVPN home page, which will make it easier for WebVPN users to access commonly used internal or external websites. Enter up to four web links to appear on the WebVPN home page, for example: `http://www.cisco.com`. In the corresponding text box, enter the name of the link as you want it to appear, for example: Cisco Systems.

Step 4 If you want to configure links to particular websites to appear on the WebVPN home page, enter the website name and URL. You can enter up to four websites.

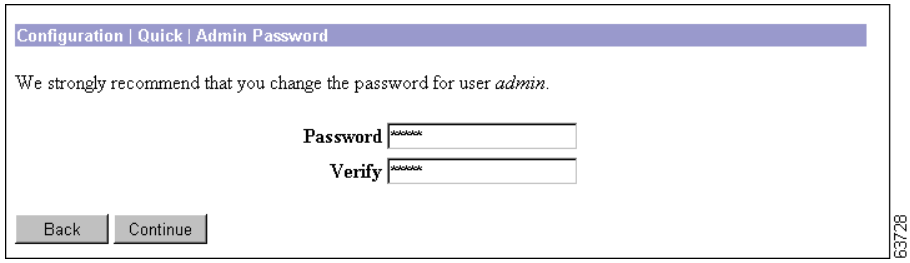
Step 5 If you want users to be able to enter their own URLs to access websites other than the ones listed on the home page, check the Allow Users to Enter URLs check box. Checking this box causes an address entry field to display on the WebVPN home page.

Step 6 Click Continue.

Changing Admin Password

The Manager displays the Configuration | Quick | Admin Password screen.

Figure 3-17 Configuration | Quick | Admin Password Screen



This screen lets you change the password for the **admin** administrator user. For ease of use during startup, the default **admin** password supplied with the VPN Concentrator is also `admin`.

Caution Since the **admin** user has full access to all management and administration functions on the device, *we strongly recommend you change this password to improve device security.*

You can further configure all administrator users on the standard Administration | Access Rights | Administrators Manager screen.

To change the password for the admin administrator user, follow these steps:

Step 1 In the Password field, enter a new password. For maximum security, the password should be at least 8 characters long, a mixture of upper- and lower-case alphabetic and numeric characters, and not easily guessed; for example, W8j9Haq3. (The field shows only asterisks.)

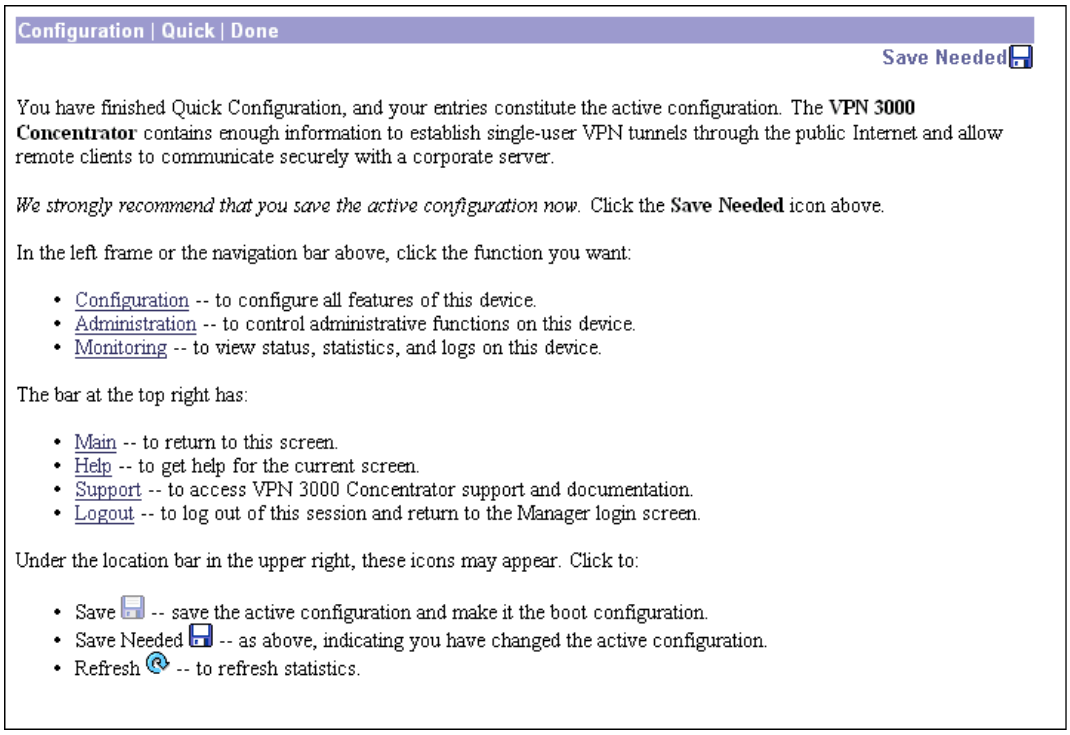
Step 2 In the Verify field, re-enter the new password to verify it.

Step 3 Click **Continue** to proceed.

Finishing Quick Configuration

The Manager displays the Configuration | Quick | Done screen.

Figure 3-18 Configuration | Quick | Done Screen


Configuration | Quick | Done
Save Needed
You have finished Quick Configuration, and your entries constitute the active configuration. The VPN 3000 Concentrator contains enough information to establish single-user VPN tunnels through the public Internet and allow remote clients to communicate securely with a corporate server.
We strongly recommend that you save the active configuration now. Click the Save Needed icon above.
In the left frame or the navigation bar above, click the function you want:
Configuration -- to configure all features of this device.
Administration -- to control administrative functions on this device.
Monitoring -- to view status, statistics, and logs on this device.
The bar at the top right has:
Main -- to return to this screen.
Help -- to get help for the current screen.
Support -- to access VPN 3000 Concentrator support and documentation.
Logout -- to log out of this session and return to the Manager login screen.
Under the location bar in the upper right, these icons may appear. Click to:
Save -- save the active configuration and make it the boot configuration.
Save Needed -- as above, indicating you have changed the active configuration.
Refresh -- to refresh statistics.
68315

You have finished quick configuration, and your entries constitute the active or running configuration. The VPN Concentrator now has enough information, and it is operational. For example, a configured remote user with a PC and modem can use Microsoft PPTP and a local ISP to connect securely—in a VPN tunnel through the Internet—with resources on a private, internal corporate network.

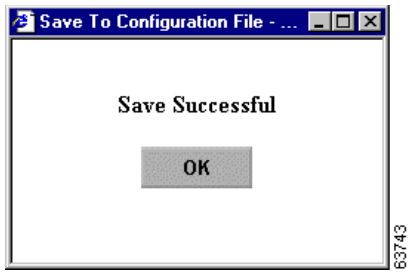
We strongly recommend that you save the active configuration before you proceed.

Saving the Active Configuration

As you make configuration entries, they take effect immediately and are included in the active, or running, configuration. *However, if you reboot the VPN Concentrator without saving the active configuration, any configuration changes are lost.*

To remind you to save your settings, the Save icon on the Manager toolbar at the top of the Manager screen changes to Save Needed as soon as the active configuration differs from the boot configuration. Click either icon to save the active configuration as the boot configuration. A pop-up window displays a status message.

Figure 3-19 Save Configuration Window



Click **OK** to close the window. Should you need to restart the VPN Concentrator, it will then boot with your configured parameters.

We strongly recommend that, as you configure the VPN Concentrator, you make it a habit to click **Save Needed** *whenever you finish setting parameters on a Manager screen.*

What Next?

Now that the VPN Concentrator is operational, you can proceed to the following functions:

- Test its operation by following the procedures under Chapter 5, "Testing the VPN Concentrator".
- Explore the Manager window and other VPN Concentrator functions. See the section "Using Other VPN Concentrator Manager Functions".
- Read a more detailed and complete system configuration. See the *VPN 3000 Series Concentrator Reference Volume I: Configuration* for assistance.

Using Other VPN Concentrator Manager Functions

To use other VPN Concentrator Manager functions, listed below, click the topic in the left frame of the Manager window or on the Manager toolbar in the top frame of the Manager window.

- Configuration—Configure all the features of the VPN Concentrator.
- Administration—Control administrative functions of this device.
- Monitoring—View status, statistics, and event logs on this device.
- Save, Save Needed—Save the active configuration and make it the boot configuration.
- Main—Return to the main Manager screen.
- Help—Open another browser window and view online help for the current Manager screen.
- Support—Open a Manager screen with links to Cisco support and documentation resources.
- Logout—Log out of this Manager session and return to the login screen.

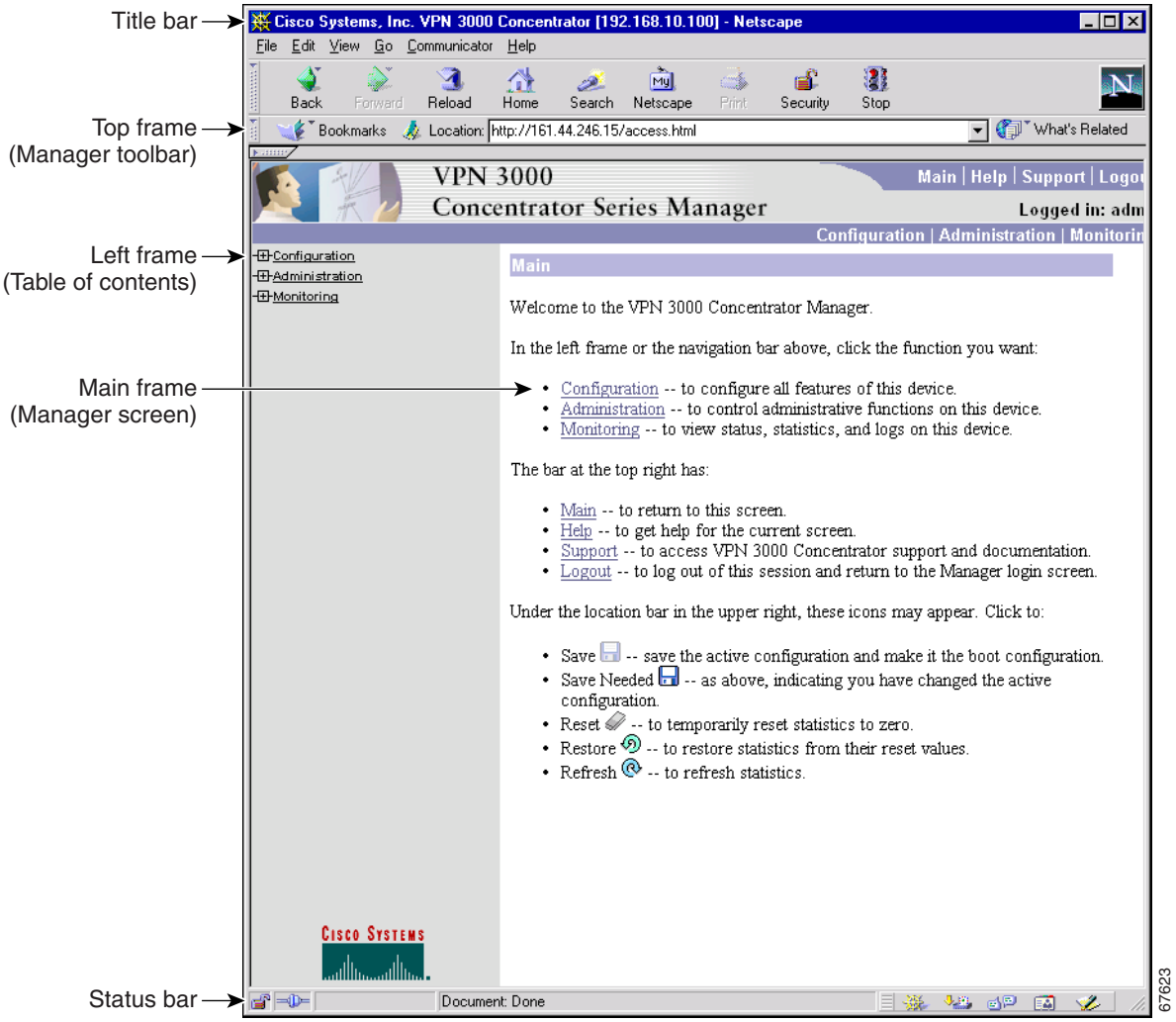
For details on the frames, functions, and icons in the Manager window, see the following section, "Understanding the VPN Concentrator Manager Window".

For details on the VPN Concentrator hardware, all the functions available in the VPN Concentrator Manager, or using the CLI, see the *VPN 3000 Concentrator Series User Guide*.

Understanding the VPN Concentrator Manager Window

The VPN Concentrator Manager window on your browser consists of three frames—top, left, and main—and it provides helpful messages and tips as you move the mouse pointer over window items. The title bar and status bar also provide useful information.

Figure 3-20 VPN Concentrator Manager Window


Title bar
Top frame
(Manager toolbar)
Left frame
(Table of contents)
Main frame
(Manager screen)
Status bar
Cisco Systems, Inc. VPN 3000 Concentrator [192.168.10.100] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://161.44.246.15/access.html What's Related
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logo
Logged in: adm
Configuration | Administration | Monitorin
Configuration
Administration
Monitoring
Main
Welcome to the VPN 3000 Concentrator Manager.
In the left frame or the navigation bar above, click the function you want:
Configuration -- to configure all features of this device.
Administration -- to control administrative functions on this device.
Monitoring -- to view status, statistics, and logs on this device.
The bar at the top right has:
Main -- to return to this screen.
Help -- to get help for the current screen.
Support -- to access VPN 3000 Concentrator support and documentation.
Logout -- to log out of this session and return to the Manager login screen.
Under the location bar in the upper right, these icons may appear. Click to:
Save -- save the active configuration and make it the boot configuration.
Save Needed -- as above, indicating you have changed the active configuration.
Reset -- to temporarily reset statistics to zero.
Restore -- to restore statistics from their reset values.
Refresh -- to refresh statistics.
Cisco Systems
Document: Done
67623

Title bar	The title bar at the top of the browser window includes the VPN Concentrator device name or IP address in brackets, for example, [10.10.4.6].
Status bar	The status bar at the bottom of the browser window displays Manager activity and explanatory messages for some items.

Mouse pointer and tips	As you move the mouse pointer over an active area, the pointer changes shape and icons change color. A description also appears in the status bar area. If you momentarily rest the pointer on an icon, a descriptive tip appears for that icon.
Top frame (Manager toolbar)	The Manager toolbar in the top frame provides quick access to Manager features. These include the following icons:
Main	Click on the **Main** tab to go to the main Manager screen, and to close all subordinate sections and titles in the left frame.
Help	Click on the **Help** tab to open context-sensitive online help. Help opens in a separate browser window that you can move or resize as you want. Close the help window when you are finished.
Support	Click on the **Support** tab to open a Manager screen with links to Cisco support and documentation resources.
Logout	Click on the **Logout** tab to log out of the Manager and return to the login screen.
Logged in: [username]	The administrator username you used to log in to this Manager session.
Configuration	Click on the **Configuration** tab to go to the main Configuration screen, to open the first level of subordinate Configuration pages in the left frame if they are not already open, and to close any open Administration or Monitoring pages in the left frame.
Administration	Click on the **Administration** tab to go to the main Administration screen, to open the first level of subordinate Administration pages in the left frame if they are not already open, and to close any open Configuration or Monitoring pages in the left frame.
Monitoring	Click on the **Monitoring** tab to go to the main Monitoring screen, to open the first level of subordinate Monitoring pages in the left frame if they are not already open, and to close any open Configuration or Administration pages in the left frame.
Save	Click on the **Save** icon to save the active configuration and make it the boot configuration. In this state, the reminder indicates that the active configuration is the same as the boot configuration, but you can save it anyway. When you change the configuration, the reminder changes to Save Needed.

Save Needed	This reminder indicates that you have changed the active configuration. Click on the **Save Needed** icon to save the active configuration and make it the boot configuration. As you make configuration entries, they take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN Concentrator without saving the active configuration, and configuration changes are lost. Clicking on this reminder saves the active configuration as the boot configuration and restores the Save reminder.
Refresh	Click on the **Refresh** icon to refresh (update) the screen contents on screens where it appears (mostly in the Monitoring section). The date and time above this reminder indicate when the screen was last updated.
Reset	Click on the **Reset** icon to reset, or start anew, the screen contents on screens where it appears (mostly in the Monitoring section).
Restore	Click on the **Restore** icon to restore the screen contents to their status prior to when you last clicked the Reset icon.
	Click on the **Cisco Systems logo** to open a browser and go to the Cisco.com web site, www.cisco.com
Left frame (Table of Contents)	On Manager screens, the left frame provides a table of contents. The table of contents uses the familiar Windows Explorer metaphor of collapsed and expanded entries.
Main section titles (Configuration, Administration, Monitoring	Click on a title to open subordinate sections and titles, and to go to that Manager screen in the main frame.
Closed or collapsed	Click on the **closed/collapsed** icon to open subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.
Open or expanded	Click on the **open/expanded** icon to close subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.
Main frame (Manager screen)	The main frame displays the current VPN Concentrator Manager screen. Many screens include a bullet list of links and descriptions of subordinate sections and titles. you can click on a link to go to that Manager screen, and open subordinate sections and titles in the table of contents.

Using the Command-Line Interface for Quick Configuration

This chapter tells you how to complete quick configuration of the system using the VPN 3000 Series command-line interface (CLI).

Quick configuration supplies the minimal parameters needed to make the VPN Concentrator operational. For example, a configured remote user with a PC and modem can use Microsoft PPTP and a local ISP to connect securely—in a VPN tunnel through the Internet—with resources on a private, internal corporate network.

The CLI is a menu-based configuration, administration, and monitoring system built into the VPN Concentrator. You can use it from the console or in a Telnet session. To use a Telnet session, connect to the IP address of the private Ethernet interface.

Before beginning the procedures in this section, you should have completed Steps 1 through 11 in the "Using the Console" section on page 2-15. As you proceed, refer to the data you recorded in Table 2-2 on page 2-13.

About Quick Configuration

The CLI has the following characteristics:

- These quick configuration menus appear only once—and you can go through the steps of quick configuration only once—unless you reboot the system with the Reboot Ignoring the Configuration File option.
- Entries are case-sensitive; for example, admin and ADMIN are different passwords.
- The system displays more tips and examples than appear in the dialogue here.
- The system shows current or default entries in brackets; for example, [10.10.4.6].
- After each entry, press the **Enter** key on the console keyboard.
- Configuration entries take effect as soon as you enter them, and they constitute the active, or running, configuration. Many quick configuration menus let you save the active configuration to the config file, and thus make it the boot configuration. We suggest you do so.
- If you make a mistake, the system displays an Error message and repeats the previous prompt. You can often enter a correct value and proceed, but in some cases you may need to restart the section to correct an earlier error. See Appendix A, "Troubleshooting and System Errors" for more details.

Configuring Ethernet Interfaces

This section describes how to configure the VPN Concentrator Ethernet interfaces.

- Ethernet 1 (Private) is the interface to your private network (internal LAN).
- Ethernet 2 (Public) is the interface to the public network.
- Ethernet 3 (External), if present, is the interface to an additional LAN.

For the VPN Concentrator to become fully operational, you must configure the two interfaces you physically connected to your network in the "Connecting Network Cables" section on page 2-9.

To configure the VPN Concentrator Ethernet Interfaces, follow these steps:

Step 1 The system prompts you to configure the VPN Concentrator interfaces.

Model 3005 Menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> _
```

Model 3015–3080 Menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Modify Ethernet 3 IP Address (External)
4) Save changes to Config file
5) Continue
6) Exit

Quick -> _
```

You entered values for Ethernet 1 under "Using the Console" section on page 2-15. You can change them now; to do so, enter **1** at the cursor. To configure another interface, enter its number at the cursor.

Step 2 We assume you enter 2 to configure Ethernet 2. The CLI displays a table with the current IP addresses and subnet masks for all three Ethernet interfaces.

```
This table shows current IP addresses.

    Interface          IP Address/Subnet Mask     MAC Address
-------------------------------------------------------------------
Ethernet 1 - Private  | 10.10.4.6/255.255.0.0 | 00.10.5A.1F.4F.07
Ethernet 2 - Public   |   0.0.0.0/0.0.0.0     |
Ethernet 3 - External |   0.0.0.0/0.0.0.0     |
-------------------------------------------------------------------

> Enter IP Address for Ethernet 2 (Public)

Quick -> [ 0.0.0.0 ] _
```

At the cursor, enter the IP address for the VPN Concentrator Ethernet 2 (Public) interface, using dotted decimal notation; for example, 192.168.12.34. Be sure no other device is using this address on the network. (Note that Ethernet 3 appears on models 3015-3080 only.)

Step 3 The system prompts you for the subnet mask for the Ethernet 2 (Public) interface. The entry in brackets is the standard subnet mask for the IP address you entered above. For example, an IP address of 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0.

```
> Enter Subnet Mask for Ethernet 2

Quick -> [ 255.255.255.0 ] _
```

At the cursor, enter the subnet mask for Ethernet 2, using dotted decimal notation; for example, 255.255.255.0. To accept the default, press **Enter**.

Step 4 The system prompts with a menu to set the speed for the Ethernet 2 interface. You can let the VPN Concentrator automatically detect and set the appropriate speed (the default), or you can set fixed speeds of 10 or 100 Mbps per second (for 10BASE-T or 100BASE-T networks). If you accept the default, be sure that the port on the active network device (hub, switch, or router) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

```
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick -> [ 3 ]
```

At the cursor, enter the menu number for your selection; for example, 1. To accept the default (3), press **Enter**.

Step 5 The system prompts with a menu to set the transmission mode for the Ethernet 2 interface. You can let the VPN Concentrator automatically detect and set the appropriate mode (the default), or you can configure the interface for full duplex (transmission in both directions at the same time) or half duplex (transmission in only one direction at a time). If you accept the default, be sure that the port on the active network device (hub, switch, or router) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.

```
1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick -> [ 1 ] _
```

At the cursor, enter the menu number for your selection; for example, 2. To accept the default (1), press **Enter**.

Step 6 The system prompts with a menu giving choices for proceeding. You can configure other interfaces, save your current entries, continue on to other quick configuration parameters, or exit the CLI. We recommend that you save first.

Model 3005 Menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Configure Expansion Cards
4) Save changes to Config file
5) Continue
6) Exit

Quick -> _
```

Model 3015–3080 Menu

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Modify Ethernet 3 IP Address (External)
4) Configure Expansion Cards
```

```
5) Save changes to Config file
6) Continue
7) Exit

Quick -> _
```

At the cursor, enter the number for Save changes to Config file.

Configuring System Information

To configure basic information that identifies your VPN Concentrator on the network, follow these steps:

Step 1 The system prompts you to assign a system name to the VPN Concentrator.

```
-- : Assign a system name to this device.

> System Name

Quick -> _
```

At the cursor, enter a name such as VPN01. This name must uniquely identify this device on your network.

Step 2 The system prompts you to specify a local DNS (Domain Name System) server, which lets you enter Internet hostnames (for example, mail01) rather than IP addresses for servers as you configure and manage the VPN Concentrator. While hostnames are easier to remember, using IP addresses avoids problems that might arise with the DNS server offline, congested, or otherwise indisposed.

```
-- : Specify a local DNS server, ...

> DNS Server

Quick -> [ 0.0.0.0 ]
```

At the cursor, enter the IP address of your local DNS server in dotted decimal notation; for example, 10.10.0.11.

Step 3 The system prompts you to enter the registered Internet domain name in which the VPN Concentrator is located (sometimes called the domain name suffix or subdomain).

```
-- : Enter your Internet domain name; ...

> Domain

Quick -> _
```

At the cursor, enter your domain name; for example, cisco.com.

Step 4 The system prompts you to specify a default gateway, which is the system to which the VPN Concentrator routes packets that are not explicitly routed. In other words, if the VPN Concentrator has no IP routing parameters (RIP, OSPF, static routes) that specify where to send packets, it will send them to this gateway. (And when you first start the VPN Concentrator, it has no IP routing parameters.)

```
> Default Gateway

Quick -> _
```

At the cursor, enter the IP address of the default gateway (for example, 10.10.0.1). This address must *not* be the same as the IP address configured on any VPN Concentrator interface. To specify no default gateway—which means the VPN Concentrator drops unrouted packets—leave this entry blank.

Configuring Tunneling Protocols and Options

This section describes how to enable, disable, and configure virtual private network tunneling protocols and encryption options on the VPN Concentrator. You *must* enable at least one of the following protocols for the device to function as a VPN device. The protocol choices are PPTP (Point-to-Point Tunneling Protocol) and L2TP (Layer 2 Tunneling Protocol), with or without Microsoft encryption required; and IPSec (IP Security protocol). PPTP and L2TP are popular with Microsoft Windows-based clients, and the Cisco VPN Client uses IPSec.

To enable, disable, and configure virtual private network tunneling protocols and encryption options on the VPN Concentrator, follow these steps:

Step 1 The system shows default settings for PPTP and L2TP—both enabled, both with no encryption required. It then prompts you to enable or disable PPTP.

```
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings

          PPTP          |         L2TP          |
------------------------------------------------
|       Enabled        |       Enabled         |
|  No Encryption Req   |  No Encryption Req    |
------------------------------------------------

1) Enable  PPTP
2) Disable PPTP

Quick -> [ 1 ]
```

At the cursor, enter **2** to disable PPTP, or press **Enter** to accept the default (1), which enables PPTP.

Step 2 If you enable PPTP, the system prompts you to select the encryption option.

- PPTP Encryption Required—PPTP connections *must* use Microsoft encryption to encrypt data. This option requires MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) and provides maximum security. During connection setup, clients must agree to use encryption or they will not be connected.
- No Encryption Required—PPTP connections *may* use Microsoft encryption to encrypt data. During connection setup, clients might or might not agree to use Microsoft encryption; they will be connected in either case.

```
1) PPTP Encryption Required
2) No Encryption Required

Quick -> [ 2 ]
```

At the cursor, enter **1** to require encryption, or press **Enter** to accept the default (2), which does not require encryption. Accept the default if you disabled PPTP.

Step 3 The system prompts you to enable or disable L2TP.

```
1) Enable  L2TP
2) Disable L2TP

Quick -> [ 1 ]
```

At the cursor, enter **2** to disable L2TP, or press **Enter** to accept the default (1), which enables L2TP.

Step 4 If you enable L2TP, the system prompts you to select the encryption option.

- L2TP Encryption Required—L2TP connections *must* use Microsoft encryption to encrypt data. This option requires MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol) and provides maximum security. During connection setup, clients must agree to use encryption or they will not be connected.
- No Encryption Required—L2TP connections *may* use Microsoft encryption to encrypt data. During connection setup, clients might or might not agree to use Microsoft encryption; they will be connected in either case.

```
1) L2TP Encryption Required
2) No Encryption Required

Quick -> [ 2 ] _
```

At the cursor, enter **1** to require encryption, or press **Enter** to accept the default (2), which does not require encryption.

Step 5 The system prompts you to enable or disable IPSec.

```
1) Enable  IPSec
2) Disable IPSec

Quick -> [ 1 ] _
```

At the cursor, enter **2** to disable IPSec, or press **Enter** to accept the default (1), which enables IPSec.

Step 6 The system prompts you to enable or disable WebVPN. WebVPN allows remote users to access the corporate network from any computer with an Internet connection to use e-mail, files, or internal websites.

```
1) Enable  WebVPN
2) Disable WebVPN

Quick -> [ 1 ] _
```

At the cursor, enter **2** to disable WebVPN, or press Enter to accept the default (1), which enables WebVPN.

Configuring Address Assignment

Configuring address assignment applies, and its menus appear, only when you enable at least one tunneling protocol. If you disabled all protocols, skip to the "Configuring Authentication" section on page 4-8.

This section lets you configure prioritized methods for assigning IP addresses to clients as a tunnel is established. The methods are configured, and used, in this order:

- Client specified—the client specifies its own IP address.

- Per user—a server assigns IP addresses on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method. (You configure an authentication server in the next section.)
- DHCP (Dynamic Host Configuration Protocol)—a DHCP server assigns IP addresses.
- Configured pool—the VPN Concentrator assigns IP addresses from an internally configured pool of addresses.

You *must* enable at least one method. You *can* enable any and all methods. By default, no method is enabled.

To configure address assignment, follow these steps:

Step 1 The system prompts you to enable or disable client-specified address assignment. If you enable IPSec, do not enable *only* this method; IPSec does not allow client-specified IP addresses.

```
-- : Configure address assignment for PPTP, L2TP and IPSec.

1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment

Quick -> [ 2 ]
```

At the cursor, enter `1` to enable client-specified address assignment, or press **Enter** to accept the default (2), disabled.

Step 2 The system prompts you to enable or disable per-user address assignment.

```
1) Enable Per User Address Assignment
2) Disable Per User Address Assignment

Quick -> [ 2 ] _
```

At the cursor, enter `1` to enable per-user address assignment, or press **Enter** to accept the default (2), disabled.

Step 3 The system prompts you to enable or disable DHCP address assignment.

```
1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment

Quick -> [ 2 ] _
```

At the cursor, enter `1` to enable DHCP address assignment, or press **Enter** to accept the default (2), disabled. If you enable DHCP, continue with the next step. If you disable DHCP, skip the next step.

Step 4 If you enable DHCP address assignment, the system prompts for the server address. If you disable DHCP, this prompt does not appear.

```
> DHCP Server

Quick -> _
```

At the cursor, enter the IP address or hostname of the DHCP server.

Step 5 The system prompts you to enable or disable configured pool address assignment.

```
1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment

Quick -> [ 2 ] _
```

At the cursor, enter **1** to enable configured pool assignment, or press **Enter** to accept the default (2), disabled. If you enable configured pool, continue with the next two steps; otherwise, skip them.

Step 6 If you enable configured pool address assignment, the system prompts for the starting IP address available in the initial pool.

```
> Configured Pool Range Start Address

Quick -> _
```

At the cursor, enter the starting IP address available in the initial configured pool. Use dotted decimal notation; for example, 10.10.1.77.

Step 7 If you enable configured pool address assignment, the system prompts for the ending IP address available in the initial pool.

```
> Configured Pool Range End Address

Quick -> [ 0.0.0.0 ] _
```

At the cursor, enter the ending IP address available in the initial configured pool. Use dotted decimal notation; for example, 10.10.1.177.

Configuring Authentication

You can choose and configure one of five types of servers to authenticate users:

- The internal VPN Concentrator authentication server
- An external RADIUS (Remote Authentication Dial-In User Service) server
- An external NT (Windows NT) Domain server
- An external SDI (RSA Security Inc. SecurID) server
- An external Kerberos/Active Directory server

You must select one authentication server type; there is no default. You can configure additional authentication servers on regular Configuration menus.

Before you configure an external server here, be sure that the external server you reference is itself properly configured and that you know how to access it (IP address or hostname, TCP/UDP port, secret/password, and so forth.). The VPN Concentrator functions as the client of these servers.

The system prompts you to select an authentication server type.

```
-- : Specify how to authenticate users.

1) Internal
2) RADIUS
3) NT Domain
4) SDI
5) Kerberos/Active Directory
6) Continue

Quick -> _
```

Step 1 At the cursor, enter the menu number for your selection; for example, 1, and skip to the step in the following section that describes your authentication server selection.

To bypass this step and continue quick configuration, enter **6**. If you enabled IPSec tunneling protocol, skip to the "Configuring the IPSec Group" section on page 4-14; otherwise skip to the "Changing the Admin Password" section on page 4-17.

Configuring Internal Authentication Server and User Database

The VPN Concentrator internal authentication server lets you enter a maximum of 100 groups and users (combined) in its database, which is adequate for a small user base. For larger numbers of users, we recommend using an external authentication server.

To use the internal server, you must create a database with at least one user, each with a user name and password, and—if you specified per-user address assignment—an IP address and subnet mask. To do so, follow these steps:

Step 1 You selected the VPN concentrator internal authentication server, and the system prompts you to add users to the internal authentication server database. When you start quick configuration, the user database is empty.

```
                                    Current Users
----------------------------------------------------------------------------
                                      No Users
----------------------------------------------------------------------------
1) Add a User
2) Delete a User
3) Continue

Quick -> _
```

At the cursor, enter **1** to add a user.

Step 2 The system prompts you to enter the user name. To be authenticated, the user must log in from the client using this name.

```
> User Name

Quick -> _
```

At the cursor, enter a unique user name; for example, simonz. The maximum is 32 characters, case-sensitive.

Step 3 The system prompts you to enter the password for this user. To be authenticated, the user must log in from the client using this password. Each user name and password combination must be unique.

```
> Password

Quick -> _
```

At the cursor, enter the user password; for example, 9se7pt14. It must be at least 8 characters long; the maximum is 32 characters, case-sensitive. The system displays only asterisks.

Step 4 The system prompts you to verify the password for this user.

```
Verify -> _
```

At the cursor, re-enter the user password. The system displays only asterisks.

If you specified per-user address assignment, continue with the next two steps. Otherwise, skip them.

Step 5 If you specified per-user address assignment, the system prompts you to enter the IP address for this user. This is the IP address assigned to this user as a client.

```
> User IP Address

Quick -> [ 0.0.0.0 ]
```

At the cursor, enter the user IP address in dotted decimal notation; for example, 10.10.1.35.

Step 6 If you specified per-user address assignment, the system prompts you to enter the subnet mask for this user. This is the subnet mask assigned to this user as a client.

```
> User Subnet Mask

Quick -> [ 0.0.0.0 ]
```

At the cursor, enter the user subnet mask in dotted decimal notation; for example, 255.255.0.0.

Step 7 The system redisplays the user database with the new user added. You can add more users, delete users, or continue with quick configuration.

```
Quick -> [ 0.0.0.0 ] 255.255.0.0

                                    Current Users
-------------------------------------------------------------------------
| 1. simonz                         |                                   |
-------------------------------------------------------------------------
1) Add a User
2) Delete a User
3) Continue

Quick -> _
```

At the cursor, enter the menu number for your selection; for example, **1**. To add more users, repeat Step 1 through Step 6 in this section. To delete a user (2), see the next step. To continue (3), skip to the "Configuring the IPSec Group" section on page 4-14 or the "Changing the Admin Password" section on page 4-17.

Step 8 If you choose to delete a user from the internal database, the system prompts you to enter the name of the user to delete.

```
> User to Delete

Quick -> _
```

At the cursor, enter the name of the existing user you want to delete; for example, simonz. You must enter the name exactly as listed in the table. After deleting the user, the system redisplays the user database as in the previous step, but without the deleted user.

Configuring RADIUS Authentication Server

External RADIUS servers can return group and user authentication parameters that match those on the VPN Concentrator; other authentication servers do not. The VPN Concentrator software CD-ROM includes a trial copy of the CiscoSecure ACS RADIUS authentication server and instructions for using it with the VPN Concentrator.

To configure an external RADIUS user authentication server, follow these steps to supply the required server IP address or hostname, server secret, and port number:

Step 1 You selected the external RADIUS authentication server, and the system prompts you to enter its hostname or IP address.

```
> RADIUS Server (Name/IP Address)

Quick ->
```

At the cursor, enter the RADIUS server hostname or IP address; for example, 192.168.56.78. The maximum length is 32 characters.

Step 2 The system prompts you to enter the RADIUS server secret, also called the shared secret, that allows access to the server.

```
> RADIUS Server Secret

Quick -> _
```

At the cursor, enter the RADIUS server secret; for example, B8y077E. The maximum length is 64 characters. The system displays only asterisks.

Step 3 The system prompts you to reenter the RADIUS server secret to verify it.

```
Verify -> _
```

At the cursor, reenter the RADIUS server secret. The system displays only asterisks.

Step 4 The system prompts you to enter the UDP port number by which you access the RADIUS server.

```
> RADIUS Server Port

Quick -> [ 0 ] _
```

At the cursor, enter the RADIUS port number; for example, 1645. To have the system supply the default port number (1645), press **Enter** to accept 0 (the default).

To continue quick configuration, skip to the "Configuring the IPSec Group" section on page 14 or the "Changing the Admin Password" section on page 4-17.

Configuring NT Domain Authentication Server

To configure an external Windows NT Domain user authentication server, follow these steps:

Step 1 You selected the external Windows NT Domain authentication server, and the system prompts you to enter its IP address.

```
> NT Domain Server Address

Quick -> _
```

At the cursor, enter the NT Domain server IP address in dotted decimal notation; for example, 192.168.56.78.

Step 2 The system prompts you to enter the NT Primary Domain Controller hostname for this server. You *must* enter this name, and it *must* be the correct hostname for the server whose IP address you entered in Step 1; if it is incorrect, authentication will fail.

```
> Primary Domain Controller

Quick -> _
```

At the cursor, enter the NT Primary Domain Controller hostname for this server; for example, PDC01. The maximum length is 16 characters.

Step 3 The system prompts you to enter the TCP port number by which you access the NT Domain server.

```
> NT Domain Server Port

Quick -> [ 0 ]
```

At the cursor, enter the NT Domain port number; for example, 139. To have the system supply the default port number (139), press **Enter** to accept 0 (the default).

To continue quick configuration, skip to the "Configuring the IPSec Group" section on page 4-14 or the "Changing the Admin Password" section on page 17.

Configuring SDI Authentication Server

To configure an external SDI (RSA Security Inc. SecurID) user authentication server, follow these steps:

Step 1 You selected the external SDI authentication server, and the system prompts you to enter its hostname or IP address.

```
> SDI Server Name

Quick -> _
```

At the cursor, enter the SDI server hostname or IP address; for example, 192.168.56.78. The maximum length is 32 characters.

Step 2 The system prompts you to enter the UDP port number by which you access the SDI server.

```
> SDI Server Port

Quick -> [ 0 ] _
```

At the cursor, enter the SDI port number; for example, 5500. To have the system supply the default port number (5500), press **Enter** to accept 0 (the default).

To continue quick configuration, proceed to the next section, "Configuring the IPSec Group," or to the "Changing the Admin Password" section on page 4-17.

Configuring Kerberos/Active Directory Authentication Server

To configure an external Kerberos/Active Directory Authentication server, follow these steps:

Step 1 You selected the Kerberos/Active Directory authentication server, and the system prompts you to enter its hostname or IP address.

```
> Kerberos Server Address/Name
Quick -->_
```

At the cursor, enter the Kerberos/Active Directory server hostname or IP address; for example, 192.168.56.78.

Step 2 The system prompts you to enter the realm name for this server, for example: US.MYCOMPANY.COM. You *must* enter this name, and it *must* be the correct realm name for the server whose IP address you entered in Step 1. If it is incorrect, authentication will fail.

The following types of servers require that you enter the realm name in all uppercase letters: Windows 2000, Windows XP, and Windows .NET. For these types of servers, if the letters are not uppercase, authentication will fail.

```
> Realm
Quick -->
```

Step 3 The system prompts you to enter the Kerberos server port number by which you access the server.

```
> Kerberos Server Port
Quick --> [0]_
```

At the cursor, enter the Kerberos server port number. To have the system supply the default port number (88), press **Enter** to accept 0 (the default).

To continue quick configuration, proceed to the next section, "Configuring the IPSec Group," or to the "Changing the Admin Password" section on page 4-17.

Configuring the IPSec Group

This section appears only if you enable the IPSec tunneling protocol.

The remote-access IPSec client connects to the VPN Concentrator via this group name and password, which are automatically configured on the internal authentication server. This is the IPSec group that creates the tunnel. Users then log in, and are authenticated, by means of their usernames and passwords.

To configure the IPSec group name and password, follow these steps:

Step 1 The system prompts you to enter the IPSec group name.

```
> IPSec Group Name

Quick -> _
```

At the cursor, enter a unique name for this group. Maximum is 32 characters, case-sensitive; for example, Group1.

Step 2 The system prompts you to enter the group password.

```
> IPSec Group Password

Quick -> _
```

At the cursor, enter a unique password for this group. The minimum is 4, and the maximum is 32 characters, case-sensitive. The system displays only asterisks.

Step 3 The system prompts you to reenter the group password to verify it.

```
Verify -> _
```

At the cursor, reenter the group password. The system displays only asterisks.

Configuring WebVPN Remote Access

The following prompts appear only if you enabled WebVPN. (See "Configuring Tunneling Protocols and Options.")

This section describes how to enable HTTPS and mail protocols for WebVPN and how to configure basic WebVPN parameters. To use any of the browser-based WebVPN features, enable HTTPS. To use e-mail proxy, enable the protocol(s) that your mail server uses: POP3S, SMTPS, or IMAP4S.

Step 1 The system prompts you to enable or disable HTTPS on the Public interface. If you did not configure the Public interface, the prompt applies to the Private interface instead.

```
Select the protocols to enable/disable on the Public interface (or Private interface if
you do not configure the Public interface), and the default system-wide e-mail servers for
WebVPN services.

1) Enable  HTTPS
2) Disable HTTPS

Quick -> [ 1 ] _
```

At the cursor, enter **2** to disable HTTPS, or press **Enter** to accept the default (1), which enables HTTPS.

Step 2 The system prompts you to enable or disable POP3S.

```
1) Enable  POP3S
2) Disable POP3S

Quick -> [ 2 ]
```

At the cursor, enter **1** to enable POP3S, or press **Enter** to accept the default (2), which disables POP3S.

If you enter **1**, the system displays the following menu:

```
> Set POP3S Default Server
Quick ->_
```

Enter the IP address of the mail server.

Step 3 The system prompts you to enable or disable SMTPS:

```
1) Enable  SMTPS
2) Disable SMTPS

Quick -> [ 2 ]
```

At the cursor, enter **1** to enable SMTPS, or press **Enter** to accept the default (2), which disables SMTPS

If you enter **1**, the system displays the following menu:

```
> Set SMTPS Default Server
Quick ->_
```

Enter the IP address of the mail server.

Step 4 The system prompts you to enable or disable IMAP4S:

```
1) Enable  IMAP4S
2) Disable IMAP4S

Quick -> [ 2 ]
```

At the cursor, enter **1** to enable IMAP4S, or press **Enter** to accept the default (2), which disables IMAP4S.

If you enter **1**, the system displays the following menu:

```
> Set IMAP4S Default Server
Quick ->_
```

Enter the IP address of the mail server.

Setting Up the WebVPN Home Page

The following prompts appear only if you enabled WebVPN. (See "Configuring Tunneling Protocols and Options.")

This section describes how to customize the home page that WebVPN users will see when they log in. You can change the title, add a banner, and configure up to four URLs.

Step 1 Enter the title to appear on each WebVPN page, for example: `My Company Remote Access`.

```
> Set WebVPN Home Page Title

Quick -> [ VPN 3000 Concentrator ]
```

Step 2 Enter a banner to appear on the WebVPN home page for the base group, for example: `Welcome to My Company Remote Access`. To keep the current value, enter a period (.) on a separate line, as shown below.

```
> Set Base Group Banner
Use '.' by itself on line to finish. Enter just a '.' to keep existing value.
->
-> .
```

Step 3 To have a link to a specific website appear on the WebVPN home page, enter the website's name. You can enter any name that users will easily recognize.

```
> Enter a descriptive name of the first HTTP/HTTPS URL

Quick ->
```

Step 4 Enter the website's URL. You can enter up to four websites/URLs.

Step 5 The system prompts you to enable users to enter their own URLs to access websites other than the ones listed on the home page. Enabling this field causes an address entry field to display on the WebVPN home page.

```
1) Enable User to Enter URLs
2) Disable User to Enter URLs

Quick -> [ 1 ]
```

At the cursor, enter **2** to disable users to enter URLS, or press **Enter** to accept the default (1), which enables it.

Changing the Admin Password

You can change the password for the admin user. For ease of use during startup, the default admin password supplied with the VPN Concentrator is also admin. Since the admin user has full access to all management and administration functions on the device, *we strongly recommend you change this password to improve device security.* You can further configure all administrators with the regular Administration menus.

Step 1 The system prompts you to change the admin password.

```
-- : We strongly recommend that you change the password ...

> Reset Admin Password

Quick -> [ ***** ] _
```

At the cursor, enter a new password for admin. Remember that entries are case sensitive. For maximum security, the password should be at least 8 characters long, a mixture of upper- and lower-case alphabetic and numeric characters, and not easily guessed; for example, W8j9Haq3. The system displays only asterisks. To keep the default, press **Enter**.

Step 2 The system prompts you to re-enter the password to verify it.

```
Verify -> _
```

At the cursor, reenter the new password. The system displays only asterisks. To keep the default, press **Enter**.

Make subsequent changes to the admin password using the VPN Concentrator Manager, on the Administration | Access Rights | Administrators | Modify Properties screen.

Completing Quick Configuration

You have finished quick configuration, and your entries constitute the active or running configuration. The VPN Concentrator now has enough information, and it is operational. For example, a configured remote user with a PC and modem can use Microsoft PPTP and a local ISP to connect securely—in a VPN tunnel through the Internet—with resources on a private, internal corporate network.

We strongly recommend that you save the active configuration before you exit. Should you need to restart the VPN Concentrator, it will then boot with your configured parameters.

Saving the Active Configuration

The system displays the final quick configuration menu.

```
1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

Quick -> 2
```

At the cursor, enter **2** to save the active configuration in the system config file.

Exiting the CLI

You are now ready to exit the CLI.

Step 1 The system redisplays the final quick configuration menu.

```
1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

Quick -> 3
```

At the cursor, enter **3** to exit the CLI.

Step 2 The system displays:

```
Done
```

If you wish to use the CLI for other functions, enter **1** at the cursor in Step 1 above. For information on using the CLI, see the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

What Next?

Now that the VPN Concentrator is operational, you can do the following:

- Test its operation by following the procedures in Chapter 5, "Testing the VPN Concentrator."
- Explore the command-line interface. The menus follow the same order, and let you perform the same functions, as the VPN Concentrator Manager. See Appendix A, "Using the Command Line Interface," in the *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* for explanations of parameters and entries.
- Explore the VPN Concentrator Manager window and other VPN Concentrator functions. See Chapter 1, "Using the VPN 3000 Concentrator Series Manager," in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.
- Proceed to a more detailed and complete system configuration. See the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

CHAPTER 5

Testing the VPN Concentrator

To test if you are able to connect to the VPN Concentrator and reach the private network, it is not necessary to install a software client. You can use either of the following methods.

- On a remote PC, connect to an ISP and use PPTP to create a secure tunnel through the Internet to the VPN Concentrator's public interface.
- Connect a PC to the network on the public side of the VPN Concentrator. Use Microsoft Dial-Up Networking to create a tunnel to the public interface of the VPN Concentrator.

This example steps you through the latter method. It uses Microsoft Dial-Up Networking on Windows 2000. If you are using a different operating system, your procedure might differ from the one shown here.

Note These instructions describe a typical installation. Please consult your ISP and your network system administrator for specific settings and instructions.

Before You Begin

To set up the test, follow these steps.

Step 1 Configure the VPN Concentrator with the following settings:

- Ethernet 2 (Public) interface with appropriate IP address (for example, 192.168.12.34) and default public filter.
- Appropriate DNS server, domain name, and default gateway.
- PPTP tunneling protocol with encryption required (MSCHAP).
- Address assignment from an appropriate configured pool of IP addresses.
- User authentication from the internal server.
- Client username (for example, simonz) and password (for example, 9se7pt14) added to the internal server user database.

Step 2 Connect a Windows 2000 PC to your network on the public side of the VPN Concentrator.

Testing the VPN Concentrator

Follow these steps to create and test a secure connection from a Windows 2000 PC client to the VPN Concentrator.

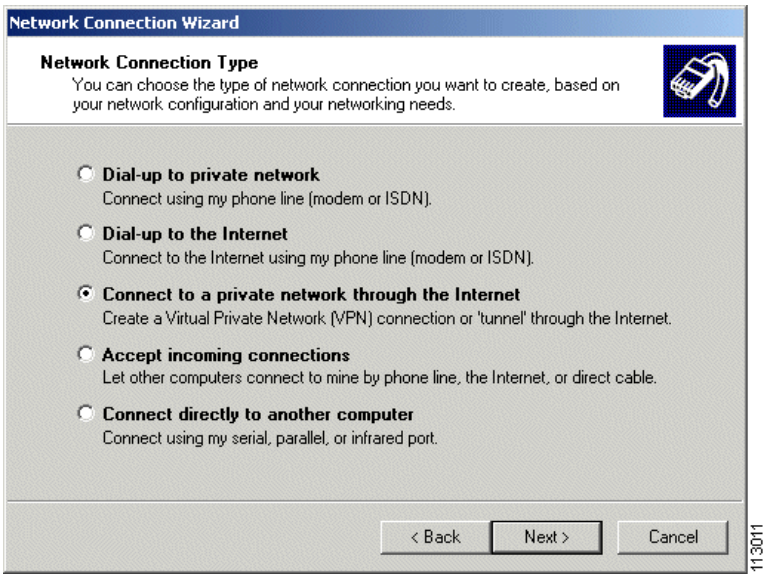
Step 1 On the client PC, choose **Start > Settings > Network and Dial-up Connections > Make a New Connection** from the Windows 2000 Start menu. The Network Connection Wizard window appears. (See Figure 5-1.)

Figure 5-1 The Network Connection Wizard Window

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel
113010

Step 2 Click **Next**. The Network Connection Type window appears. (See Figure 5-2.)

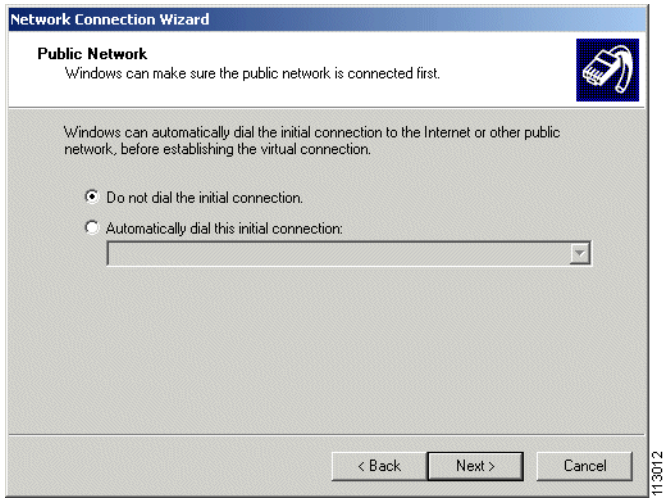
Figure 5-2 Network Connection Type Window


Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel
113011

Step 3 Choose **Connect to a private network through the Internet**.

Step 4 Click **Next**. The Public Network window appears. (See Figure 5-3.)

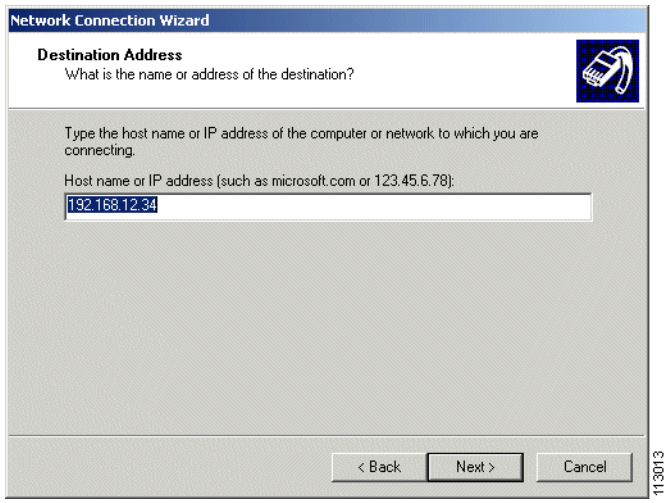
Figure 5-3 Public Network Window


Network Connection Wizard
Public Network
Windows can make sure the public network is connected first.
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.
Do not dial the initial connection.
Automatically dial this initial connection:
< Back
Next >
Cancel
113012

Step 5 Choose **Do Not Dial the Initial Connection**.

Step 6 Click **Next**. The Destination Address window appears. (See Figure 5-4.)

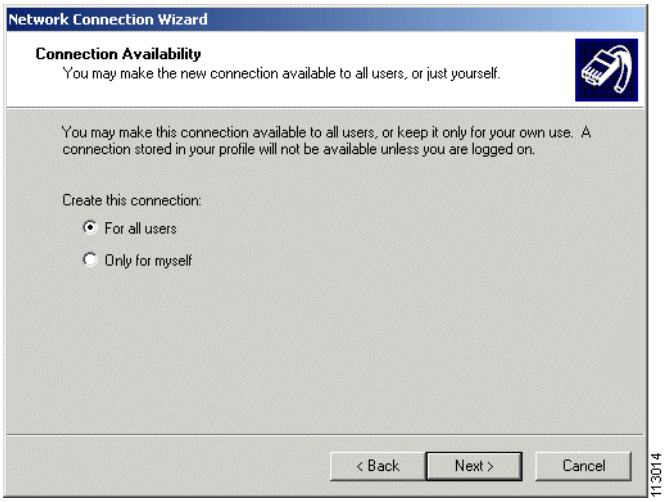
Figure 5-4 Destination Address Window


Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
192.168.12.34
< Back
Next >
Cancel
113013

Step 7 Enter the public interface address of your VPN Concentrator.

Step 8 Click **Next**. The Connection Availability window appears. (See Figure 5-5.)

Figure 5-5 Connection Availability Window


Network Connection Wizard
Connection Availability
You may make the new connection available to all users, or just yourself.
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.
Create this connection:
For all users
Only for myself
< Back
Next >
Cancel
113014

Step 9 Choose **For all Users**.

Step 10 Click **Next**. The Completing the Network Connection Wizard window appears. (See Figure 5-6.)

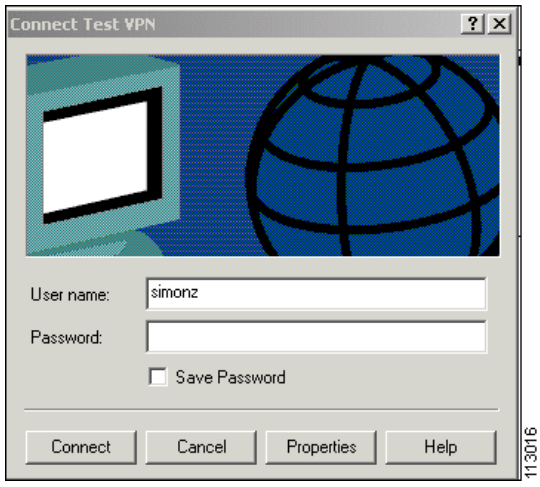
Figure 5-6 Completing the Network Connection Wizard Window

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Test VPN
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel
113015

Step 11 Enter a name for the connection, for example: `TestVPN`.

Step 12 Click **Finish**. The Connect window appears. (See Figure 5-7.)

Figure 5-7 Connect Window

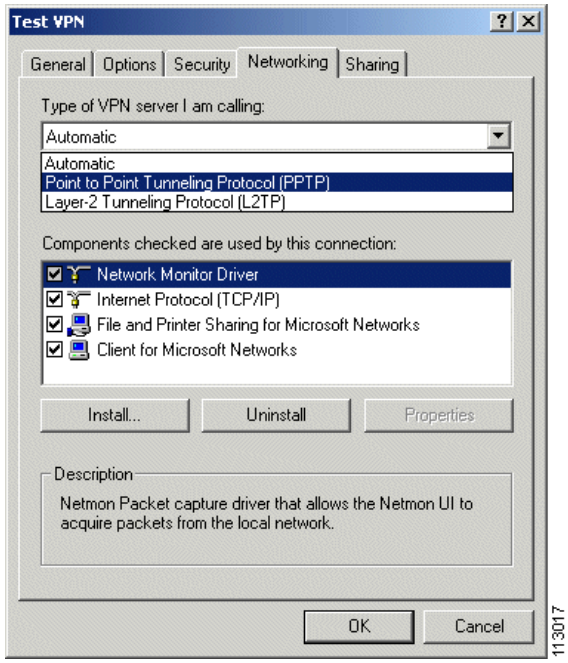


Step 13 Enter the username you previously added to the internal server user database. (See "Before You Begin.")

Step 14 Click the **Properties** button. The Properties dialog box appears.

Step 15 Choose the **Networking** tab.

Figure 5-8 Properties Dialog Box, Networking Tab

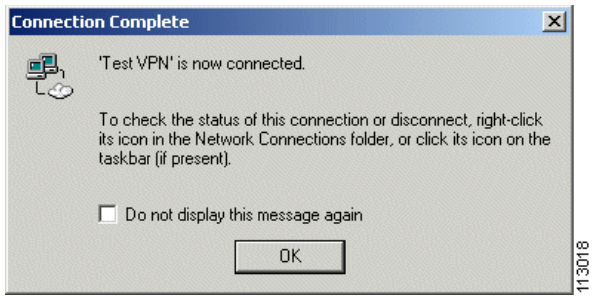


Step 16 Select **Point to Point Tunneling Protocol (PPTP)** from the Type of VPN Server I am Calling drop-down menu. (See Figure 5-8.) Click **OK**. The Properties dialog box disappears.

Step 17 In the Connect window, enter the password.

Step 18 Click **Connect**. If the connection is successful, the Connection Complete window appears. (See Figure 5-9.) The PC is now connected to the VPN Concentrator via a secure PPTP connection.

Figure 5-9 Connection Complete


Connection Complete
'Test VPN' is now connected.
To check the status of this connection or disconnect, right-click its icon in the Network Connections folder, or click its icon on the taskbar (if present).
Do not display this message again
OK
113018

Step 19 Click OK to dismiss the window.

If you receive an error message, check your connections and VPN Concentrator settings, then run the test again.

Troubleshooting and System Errors

Appendix A describes common errors that can occur while configuring and using the system, and how to correct them. It also describes LED indicators on the system and its expansion modules.

Files for Troubleshooting

The VPN 3000 Concentrator creates several files that you can examine and that can assist Cisco support engineers when troubleshooting errors and problems:

- Event log
- SAVELOG.TXT—Event log that is automatically saved when the system crashes and when it is rebooted
- CRSHDUMP.TXT—Internal system data file that is written when the system crashes
- CONFIG, CONFIG.BAK—Normal configuration file used to boot the system, and backup configuration file

Event Logs

The VPN Concentrator records system events in the event log, which is stored in nonvolatile memory (NVRAM). To troubleshoot operational problems, we recommend that you start by examining the event log. See Configuration | System | Events and Monitor | Event Log.

The VPN Concentrator automatically saves the event log to a file in flash memory if it crashes, and when it is rebooted. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging. See Configuration | System | Events and Administration | File Management | Files.

Crash Dump File

If the VPN Concentrator crashes during operation, it saves internal system data in nonvolatile memory (NVRAM), and then automatically writes this data to a CRSHDUMP.TXT file in flash memory when it is rebooted. This file contains the crash date and time, software version, tasks, stack, registers, memory, buffers, and timers., which are helpful to Cisco support engineers. In case of a crash, we ask that you send this file when you contact Technical Assistance Center (TAC) for assistance. See Administration | File Management | Files for information on managing files in flash memory.

Configuration Files

The VPN Concentrator saves the current boot configuration file (CONFIG) and its predecessor (CONFIG.BAK) as files in flash memory. These files may be useful for troubleshooting. See Administration | File Management | Files for information on managing files in flash memory.

VPN Concentrator Manager Errors

Table A-1 lists errors that might occur while using the HTML-based VPN Concentrator Manager with a browser.

Table A-1 VPN Concentrator Manager Errors

Symptom	Problem	Possible Cause	Solution
Browser Refresh or Reload Button Logs Out the Manager.	You clicked the **Refresh** or **Reload** button on the *browser* navigation toolbar, and the Manager logged out. The main login screen appears.	To protect access security, clicking **Refresh / Reload** on the browser toolbar automatically logs out the Manager session.	Do not use the browser navigation toolbar buttons with the VPN Concentrator Manager. Use only the Manager **Refresh** button where it appears on a screen. We recommend that you hide the browser navigation toolbar to prevent mistakes.
Browser Back or Forward Button displays an Incorrect Screen or Incorrect Data.	You clicked the **Back** or **Forward** button on the *browser* navigation toolbar, and the Manager displayed the wrong screen or incorrect data.	To protect security and the integrity of data entries, clicking **Back** or **Forward** on the browser toolbar deletes pointers and values within the Manager.	Do not use the browser navigation toolbar buttons with the VPN Concentrator Manager. Navigate using the location bar at the top of the Manager window, the table of contents in the left frame, or links on Manager screens. We recommend that you hide the browser navigation toolbar to prevent mistakes.
The Manager displays the Invalid Login or Session Timeout screen.	You entered an invalid administrator login name and password combination.	• Typing error • Invalid (unrecognized) login name or password.	Reenter the login name and password and click **Login**. Use a valid login name and password. Type carefully.

Table A-1 VPN Concentrator Manager Errors (continued)

Symptom	Problem	Possible Cause	Solution
The Manager displays the Invalid Login or Session Timeout screen.	The Manager session has been idle longer than the configured timeout interval. (The default timeout interval is 600 seconds (10 minutes).)	• No activity for (interval) seconds. The Manager resets the inactivity timer only when you click an action button (such as **Apply**, **Add**, or **Cancel**) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen *does not* reset the timer. • Timeout interval set too low for normal use.	On the Administration | Access Rights | Access Settings screen, change the Session Timeout interval to a larger value and click **Apply**.
The Manager displays a screen with the message, "Error/ An error has occurred while attempting to perform the operation." An additional error message describes the erroneous operation.	You tried to perform an operation that is not allowed.	The screen displays a message that describes the cause.	Click **Retry the operation** to return to the screen where you were working and correct the mistake. Carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost. Click **Go to main menu** to go to the main Manager screen.
The Manager displays a screen with the message, "You are using an old browser or have disabled JavaScript..."	The VPN Concentrator Manager cannot work with the browser that you have invoked.	• You are using the Manager with an unsupported browser. • You are using the Manager with an obsolete browser. • You are using a browser that does not have JavaScript enabled.	Use Microsoft Internet Explorer version 4.0 or higher. Use Netscape Navigator version 4.5 or higher. Be sure JavaScript is enabled in the browser. (See the "Browser Requirements" section on page 2-2 of this manual.)

Table A-1 VPN Concentrator Manager Errors (continued)

Symptom	Problem	Possible Cause	Solution
The Manager displays a screen with the message, "Not Allowed/You do not have sufficient authorization to access the specified page."	You tried to access an area of the Manager that you do not have authorization to access.	• You logged in using an administrator login name that has limited privileges. • You logged in from a workstation that has limited access privileges.	Log in using the system administrator login name and password. (Defaults are `admin`/`admin`.) Log in from a workstation with greater access privileges. Have the system administrator change your privileges on the Administration | Access Rights | Administrators screen. Have the system administrator change the privileges of your workstation on the Administration | Access Rights | Access Control List screen.
The Manager displays a screen with the message, "Not Found / An error has occurred while attempting to access the specified page." The screen includes additional information that identifies system activity and parameters.	The Manager could not find a screen.	• You updated the software image and did not clear the browser's cache.	Clear the browser cache: delete its temporary internet files, history files, and location bar references. Then try again.
		• There is an internal Manager error.	Please note the system information on the screen and contact TAC for assistance.
Microsoft Internet Explorer displays a Script Error dialog box that includes the error message, "No such interface supported."	While using a Manager function that opens another browser window (such as Save Needed, Help, or Software Update), Internet Explorer cannot open the window and displays the error dialog box.	A bug in the Internet Explorer JavaScript interpreter.	1. Click **No** on the error dialog box. 2. Log out of the Manager. 3. Close Internet Explorer. 4. Reinstall Internet Explorer.

Command-line Interface Errors

Table A-2 lists errors that might occur while using the menu-based Command-line Interface from a console or Telnet session.

Table A-2 VPN 3000 Concentrator Command-Line Interface Errors

Console Message	Problem	Possible Cause	Solution
ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID.	The system expected a valid 4-byte dotted decimal entry, and the entry wasn't in that format.	• You entered something other than a 4-byte dotted decimal number. You might have omitted a byte position, or entered a number greater than 255 in a byte position. • You entered `0.0.0.0` instead of an appropriate address.	At the prompt, reenter a valid 4-byte dotted decimal number.
ERROR:-- Out of Range Value Entered. Try Again.	The system expected a number within a certain range, and the entry was outside that range.	• You entered a letter instead of a number. • You entered a number greater than the possible menu numbers.	At the prompt, reenter a number in the appropriate range.
ERROR:-- The Passwords Do Not Match. Please Try Again.	The entry for a password and the entry to verify the password do not match.	• You mistyped an entry. • You entered either a password or verify entry, but not the other.	At the Verify prompt, re-enter the password. If the original password is incorrect, press **Enter** and re-enter both the password and the verification at the prompts.

LED Indicators

LED indicators on the VPN Concentrator and its expansion modules are normally green. The usage gauge LEDs are normally blue. LEDs that are amber or off might indicate an error condition. NA means not applicable; that is, the LED does not have that state.

Contact TAC if any LED indicates an error condition.

VPN Concentrator (front) LEDs

The LEDs on the front of the VPN 3000 Concentrator are as follows:

LED Indicator	Green	Amber	Off
System	Power on. Normal Blinking Green (Model 3005 only)—System is in a shutdown (halted) state, ready to power off.	System has crashed and halted. *Error.*	Power off. (All other LEDs are also off.)
The LEDs below exist only on Models 3015–3080			
Ethernet Link Status 1 2 3	Connected to network and enabled. Blinking Green—Connected to network and configured, but disabled.	NA	Not connected to network or not enabled.
Expansion Modules Insertion Status 1 2 3 4	SEP or SEP-E module installed in system.	NA	Module not installed in system.
Expansion Modules Run Status 1 2 3 4	SEP or SEP-E module operational.	Module failed during operation. *Error.*	If installed, module failed diagnostics or encryption code is not running. *Error.*
Fan Status	Operating normally.	Not running or RPM below normal range. *Error.*	NA
Power Supplies A B	Installed and operating normally.	Voltage(s) outside of normal ranges. *Error.*	Not installed.
CPU Utilization	This statistic selected for usage gauge display.	NA	Not selected.
Active Sessions	This statistic selected for usage gauge display.	NA	Not selected.
Throughput	This statistic selected for usage gauge display.	NA	Not selected.

Usage Gauge LEDs ***(Models 3015–3080 only)***	**Steady or Intermittent Blue**	**Blinking Blue**
Left to right sequential segments, varying number	Normal operation.	NA
All 10 segments	NA	VPN Concentrator is in a shutdown (halted) state, ready to power off.

VPN Concentrator Rear LEDs

The LEDs on the rear of the VPN 3000 Concentrator are as follows:

LED Indicator	Green	Amber	Off
Private / Public / External Ethernet Interfaces (connected to network)			
Link	Carrier detected. Normal.	NA	No carrier detected. *Error.*
Tx	Transmitting data. Normal. Intermittent on.	NA	Not transmitting data. Idle. Intermittent off.
Coll	NA	Data collisions detected.	No collisions. Normal.
100	Speed set at 100 Mbps.	NA	Speed set at 10 Mbps.

SEP Module LEDs

SEP (Scalable Encryption Processing) module LEDs are present only on models 3015 through 3080 and are visible from the rear of the VPN Concentrator.

SEP Module LED	Green	Amber	Off
Power	Power on. Normal.	NA	Power is not reaching the module. It might not be seated correctly. *Error.*
Status (SEP only)	Encryption code is running. Normal.	SEP module failed during operation. *Error.*	SEP module failed diagnostics or encryption code is not running. *Error.*
Activity (SEP-E only)	Encryption code is running. Normal.	SEP-E module failed during operation. *Error.*	SEP-E module failed diagnostics or encryption code is not running. *Error.*

Copyrights, Licenses, and Notices

Software License Agreement of Cisco Systems, Inc.

CISCO SYSTEMS, INC. IS WILLING TO LICENSE TO YOU THE SOFTWARE CONTAINED IN THE ACCOMPANYING CISCO PRODUCT ONLY IF YOU ACCEPT ALL OF THE TERMS AND CONDITIONS IN THIS LICENSE AGREEMENT. PLEASE READ THIS AGREEMENT CAREFULLY BEFORE YOU OPEN THE PACKAGE BECAUSE, BY OPENING THE SEALED PACKAGE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CISCO SYSTEMS WILL NOT LICENSE THIS SOFTWARE TO YOU. IN THAT CASE YOU SHOULD RETURN THE PRODUCT PROMPTLY, INCLUDING THE PACKAGING, THE UNOPENED PACKAGE, ALL ACCOMPANYING HARDWARE, AND ALL WRITTEN MATERIALS, TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Ownership of the Software

1. The software contained in the accompanying Cisco VPN 3000 Concentrator and any accompanying written materials are owned or licensed by Cisco Systems and are protected by United States copyright laws, laws of other nations, and/or international treaties.

Grant of License

2. Cisco Systems hereby grants to you the right to use the Software with the Cisco VPN 3000 Concentrator product. To this end, the Software contains both operator software for use by the network administrator and client software for use by clients at remote network nodes. You may transfer the client software, or portions thereof, only to prospective nodes on the network, and to no one else. You may not transfer the operator software.

Restrictions on Use and Transfer

3. You may not otherwise copy the Software, except that you may make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single disk provided you keep the disk solely for backup or archival purposes. You may not copy the written materials and you may not use the backup or archival copy of the Software except in conjunction with the accompanying Cisco product.

4. You may permanently transfer the Software and accompanying written materials (including the most recent update and all prior versions) only in conjunction with a transfer of the entire Cisco product, and only if you retain no copies and the transferee agrees to be bound by the terms of this Agreement. Any transfer terminates your license. You may not rent or lease the Software or otherwise transfer or assign the right to use the Software, except as stated in this paragraph.

5. You may not export the Software, even as part of the Cisco product, to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software, even as part of the Cisco product, in violation of any export control laws of the United States or any other country.

6. You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or accompanying documentation or any copy thereof, in whole or in part.

7. The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy, or return to Cisco Systems, the Software and accompanying documentation and all copies thereof. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.

8. You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 and 3 hereof.

9. You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.

10. Any notice, demand, or request with respect to this Agreement shall be in writing and shall be effective only if it is delivered by hand or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to Cisco Systems, whose address is set forth below. Such communications shall be effective when they are received by Cisco Systems.

Limited Warranty

11. Cisco Systems warrants that the Software will perform substantially in accordance with the accompanying written materials for a period of 90 days from the date of your receipt of the Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

12. CISCO SYSTEMS DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING WRITTEN MATERIALS, AND THE ACCOMPANYING HARDWARE. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

13. CISCO SYSTEMS' ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY SHALL BE, AT CISCO SYSTEMS' CHOICE, EITHER (A) RETURN OF THE PRICE PAID OR (B) REPLACEMENT OF THE SOFTWARE THAT DOES NOT MEET CISCO SYSTEMS' LIMITED WARRANTY AND WHICH IS RETURNED TO CISCO SYSTEMS TOGETHER WITH A COPY OF YOUR RECEIPT. Any replacement Software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. These remedies are not available outside the United States of America.

14. This Limited Warranty is void if failure of the Software has resulted from modification, accident, abuse, or misapplication.

15. IN NO EVENT WILL CISCO SYSTEMS BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY LOSS OF PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE SOFTWARE. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

16. This Agreement is governed by the laws of the State of Massachusetts.

17. If you have any questions concerning this Agreement or wish to contact Cisco Systems for any reason, please call (508) 553-8621, or write to

Cisco Systems, Inc.
124 Grove Street, Suite 205
Franklin, Massachusetts 02038.

18. U.S. Government Restricted Rights. The Software and accompanying documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c)(1) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1)(ii) and (2) of Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Supplier is Cisco Systems, Inc., 124 Grove Street, Suite 205, Franklin, Massachusetts 02038.

19. This Agreement constitutes the entire agreement between Cisco Systems and the licensee. There are no understandings, agreements, representations, or warranties, expressed or implied, not specified herein regarding this Agreement or the Software licensed hereunder. Only the terms and conditions contained in this Agreement shall govern the transaction contemplated hereunder, notwithstanding any additional, different, or conflicting terms which may be contained in any purchase order or other documents pertaining to the subject transaction.

Other Licenses

The VPN 3000 Concentrator Series contains and uses software from other firms, under license. Relevant copyright and license notices follow.

BSD Software

Copyright © 1990, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DHCP Client

Copyright © 1995, 1996, 1997 The Internet Software Consortium.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of The Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DNS Resolver (Client)

DNS Resolver / BSD / DEC / Internet Software Consortium

Copyright © 1988, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright © 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED “AS IS” AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission.

To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product.

THE SOFTWARE IS PROVIDED “AS IS”, AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

IPSec

COPYRIGHT1.1a (NRL) 17 August 1995

COPYRIGHT NOTICE

All of the documentation and software included in this software distribution from the US Naval Research Laboratory (NRL) are copyrighted by their respective developers.

This software and documentation were developed at NRL by various people. Those developers have each copyrighted the portions that they developed at NRL and have assigned All Rights for those portions to NRL. Outside the USA, NRL also has copyright on the software developed at NRL. The affected files all contain specific copyright notices and those notices must be retained in any derived work.

NRL LICENSE

NRL grants permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation created at NRL provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed at the Information Technology Division, US Naval Research Laboratory.

4. Neither the name of the NRL nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THE SOFTWARE PROVIDED BY NRL IS PROVIDED BY NRL AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO FINISHED SHALL NRL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the US Naval Research Laboratory (NRL).

LDAP

Copyright © 1992-1996 Regents of the University of Michigan.
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty.

LZS221-C v6

Copyright © 1988-1999 by Hi/fn, Inc. Includes one or more U.S. Patent numbers: 4701745, 5016009, 5126739, 5146221, 5414425, 5463390, and 5506580. Other Patents Pending.

MPPC-C v4

Copyright © 1996-1998 by Hi/fn, Inc. Includes one or more U.S. Patent numbers: 4701745, 5016009, 5126739, 5146221, 5414425, and 5463390. Other Patents Pending.

Outline Style Table of Contents in JavaScript

OUTLINE STYLE TABLE OF CONTENTS in JAVASCRIPT, Version 3.0
by Danny Goodman (dannyg@dannyg.com)
Analyzed and described at length in “JavaScript Bible”, by Danny Goodman
(IDG Books ISBN 0-7645-3022-4)

This program is Copyright 1996, 1997, 1998 by Danny Goodman. You may adapt this outline for your Web pages, provided these opening credit lines (down to the lower dividing line) are in your outline HTML document. You may not reprint or redistribute this code without permission from the author.

RSA Software

Copyright © 1995-1998 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

BSAFE is a trademark of RSA Data Security, Inc.

SecureID

SecureID is a product of RSA Security Inc., Bedford, MA. (formerly Security Dynamics Technologies, Inc.)

Use of SDTI's Trade Name and Trademarks

(a) Any advertising or promotional literature or announcement to the press by the Partner regarding its relationship with SDTI, or otherwise utilizing SDTI's name or trademarks must be approved by SDTI in writing in advance, which approval will not be unreasonably withheld or delayed.

(b) The Partner shall include and shall not alter, obscure or remove any SDTI name or any other trademark or trade name used by SDTI or any markings, colors or other insignia which are contained on or in or fixed to the Software (collectively, “Proprietary Marks”). Partner agrees to include SDTI's copyright notice in its help screen as it pertains to the SDTI Translation.

Server SNMP

Copyright 1998 by Carnegie Mellon University
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Client SNMP

Copyright © 1996, 1997 by Westhawk Ltd.(www.westhawk.co.uk)

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation. This software is provided “as is” without express or implied warranty.

author tpanton@ibm.net (Tim Panton)

SSH

Copyright © 1993, 1995-2000 by DataFellows, Inc. All rights reserved.

SSL Plus

Certicom, the Certicom logo, SSL Plus, and Security Builder are trademarks of Certicom Corp. Copyright © 1997-1999 Certicom Corp. Portions are Copyright © 1997-1998, Consensus Development Corporation, a wholly owned subsidiary of Certicom Corp. All rights reserved.

Contains an implementation of NR signatures, licensed under U.S. patent 5,600,725. Protected by U.S. patents 5,787,028; 4,745,568; 5,761,305. Patents pending.

TCP Compression / Uncompression

Routines to compress and uncompress TCP packets (for transmission over low speed serial lines).

Copyright © 1989 Regents of the University of California.
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Van Jacobson (van@helios.ee.lbl.gov), Dec 31, 1989:
- Initial distribution.

Modified for KA9Q Internet Software Package by Katie Stevens (dkstevens@ucdavis.edu)
University of California, Davis
Computing Services

- 01-31-90initial adaptation (from 1.19)
PPP.0502-15-90 [ks]
PPP.0805-02-90 [ks]use PPP protocol field to signal compression
PPP.1509-90 [ks]improve mbuf handling
PPP.1611-02 [karn]substantially rewritten to use NOS facilities

- Feb 1991Bill_Simpson@um.cc.umich.edu
variable number of conversation slots
allow zero or one slots
separate routines
status display

Telnet Server

Copyright phase2 networks 1996. All rights reserved.

SID: 1.1

Revision History:
1.197/06/23 21:17:43 root

Regulatory Standards Compliance

Standards Compliance

The VPN 3000 Concentrator complies with the following regulatory standards:

Specification	Description
Regulatory compliance	Products bear CE Marking indicating compliance with (99/5/EEC) directives, which includes the following safety and EMC standards.
Safety	UL 60950 CAN/CSA-C22.2 No. 60950 EN 60950 IEC 60950 TS 001 AS/NZS 3260

Specification	Description
EMC	FCC Part 15 (CFR 47) Class A ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI Class A EN55024 ETS300 386-2 EN50082-1 EN61000-3-2 EN61000-3-3
Telecom (E1)	CTR 12/13 ACA TS016
Telecom (T1)	US FCC Part 68 Canadian CS03 JATE Green Book

FCC Part 68 Notice

The equipment complies with Part 68 of the FCC rules. On the tray of this equipment is a label that contains, among other information, the FCC registration number. If requested, this information must be provided to the telephone company.

This equipment cannot be used on telephone company-provided coin services. Connection to the Party Line Service is subject to state tariffs.

If this equipment causes harm to the telephone network, the telephone company notifies you in advance that temporary discontinuance of service might be required. If advance notice is not practical, the telephone company notifies the customer as soon as possible. Also, you are advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company can make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company provides advance notice in order for you to make the necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact us for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company can request you remove the equipment from the network until the problem is resolved.

We recommend that you install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightning strikes and other electrical surges.

This equipment uses the Uniform Service Order Code (USOC) jacks described below.

Model Name	Facility Interface Code	Service Order Code	Jack Type
CVPN_3000-2T	04DU9-1SN	6.0N	RJ48C

CS-03 Certification

The equipment is CS-03 certified. Refer to Table B-1 for CS03 approval details for equipment. Observe the following general information and safety precautions:

The industry Canada label identifies CS-03 certified equipment. This certification means that the equipment meets certain telecommunications network protection, operation, and safety requirements as described in the appropriate terminal equipment requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing the equipment, ensure that it is permissible to connect them to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning **Do not attempt to make such connections yourself. Contact the appropriate electric inspection authority or electrician as appropriate.**

Table B-1 CS03 Approval

Model Number	Approval Number
CVPN3005-T1	#2461 10854 A
CVPN3000-2T1	#2461 10854 A

JATE

The equipment meets the requirements of the Japan Approvals Institute for Telecommunications Equipment (JATE). Refer to Table B-2 for JATE approval details.

Table B-2 JATE Approval

Applicant Name	Model Number	Approval Number
Nihon Cisco Systems	CVPN3000-2T1	#D00-0687 JP
Nihon Cisco Systems	CVPN3005-T1	#D00-0687 JP

EMC Environmental Conditions for Product to be Installed in the European Union

This equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under user's control.
- Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
- Where applicable, AC power distribution shall be one of the following types: TN-S and TN-C [as defined in IEC 364-3]

In addition, if equipment is operated in a domestic environment, interference might occur.

(FCC) Class A Warning

"Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense."

[cfr reference 15.21]

For Class A equipment

"NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense."

[cfr reference 15.105]

Canada Class A Warning

This Class 'A' digital apparatus complies with Canadian ICES-003.
Cet appareil numerique de la classe 'A' e_t conforme á la norme NMB-003 de Canada.

(CISPR 22) Class A Warning

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Japan (VCCI) Class A Warning

これは、情報処理装置等電波障害自主規制協議会（VCCI）の規定に基づくクラスA装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を取るように要求されることがあります。

Translation:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Hungarian Class A Warning

Warning **This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.**

Figyelem **Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.**

Numerics

100 LED (Ethernet) A-7

A

access to device, physical 2-2
active configuration
  definition 3-3, 4-1
  saving 4-18
Active Sessions LED A-6
Activity LED for SEP-E A-7
adding a user 3-17, 4-9
address assignment, configuring 3-10, 4-6
administrator requirements 2-1
admin password
  changing 4-17
  configuring 3-21
  default 3-21, 4-17
authentication
  algorithms 1-4
  configuring 3-11, 4-8
  internal server 3-11, 4-9
  Kerberos/Active Directory 3-16, 4-13
  NT Domain 3-14, 4-12
  RADIUS 3-13, 4-11
  SDI 3-15, 4-12
  supported servers 1-5, 4-8

B

Back button 3-3
Bad IP Address error A-5
bandwidth management 1-7
beginning quick configuration 2-12
bootcode, upgrading viii
boot messages at startup 2-11
brackets, default entries in 4-1
browser
  Back or Forward button displays incorrect screen or incorrect data A-2, A-3
  navigation toolbar, don't use with Manager 3-3
  navigation toolbar not used with Manager 2-3
  Refresh / Reload button logs out the Manager A-2, A-5
  requirements 2-2
  starting 3-1

C

cables and connectors
  connecting 2-9
  distance specifications 1-9
  requirements 2-2
case-sensitivity 3-3, 4-1
Certificate Authorities supported 1-5
changing admin password 4-17
CiscoSecure ACS server 3-12, 4-11
CLI
  errors A-5
  exiting 4-18
  Quick Configuration using 4-1
client software compatibility features 1-7
client specified address assignment 4-7
clustering features 1-6
Coll LED (Ethernet) A-7
Command-Line Interface

See CLI
compliance standards B-10
configuration
  active or running 3-3, 4-1
  quick *See* Quick Configuration 4-1
configuration files
  for troubleshooting A-2
  saving 2-17, 3-22, 3-23, 4-18
configuring 4-12, 4-13
  address assignment 3-10, 4-6
  authentication 3-11, 4-8
  Ethernet interfaces 3-4, 4-2
  internal authentication server 3-12, 4-9
  internal server user database 4-9
  IPSec Group 3-18, 4-14
  Kerberos/Active Directory authentication server 3-16, 4-13
  NT Domain authentication server 3-14, 4-12
  RADIUS authentication server 3-12, 4-11
  remote access 3-19, 3-20, 4-14, 4-16
  SDI authentication server 3-15, 4-12
  system information 3-8, 4-4
  tunneling protocols and options 3-9, 4-5
  WebVPN 3-19
connecting
  console 2-8
  network cables 2-9
  power cable 2-9
console
  connecting 2-8
  requirements 2-2
  to start quick configuration 2-15
conventions, documentation viii
cooling
  requirements 2-1
  specifications 1-8
copyrights and licenses B-1
CPU Utilization LED A-6
crash, system
  saves log file A-1
CRSHDUMP.TXT file A-1

D

data compression 1-7
data formats xi
date, setting 2-15, 3-8
Daylight-Saving Time, enabling 2-16, 3-8
default
  admin password 3-21, 4-17
  CLI entries 4-1
  gateway 3-9, 4-4
  login password 2-15
deleting a user 3-18, 4-10
DHCP address assignment 3-11, 4-7
digital Certificate Authorities supported 1-5
display settings 2-3
documentation
  cautions x
  conventions viii
  notes x
  related viii
  tips x
DST, *See* Daylight-Saving Time 2-16
duplex transmission 3-7, 4-3

E

encryption
  algorithms 1-4
  options, configuring 3-9, 4-5
errors
  and troubleshooting A-1
  an error has occurred ... A-3
  bad IP address A-5
  CLI A-5
  insufficient authorization A-4

- invalid login A-2, A-3
- JavaScript A-3
- messages 3-3
- no such interface supported (IE) A-4
- not allowed A-4
- not found A-4
- old browser A-3
- out of range value A-5
- passwords do not match A-5
- recovering from 3-3
- session timeout A-2, A-3
- VPN Concentrator Manager A-2

Ethernet interfaces
- configuring 4-2
- modifying 3-5

Ethernet Link Status LEDs A-6

event log
- saved at system reboot A-1
- saved if system crashes A-1

exiting the Command-Line Interface 4-18

Expansion Modules
- Insertion Status LEDs A-6
- Run Status LEDs A-6

F

Fan Status LED A-6

features
- hardware 1-2
  - Model 3005 1-2
  - Model 3015 1-2
  - Model 3020 1-2
  - Model 3030 1-3
  - Model 3060 1-3
  - Model 3080 1-3
- software
  - authentication algorithms 1-4
  - bandwidth management 1-7
  - client compatibility 1-7
  - clustering 1-6
  - data compression 1-7
  - digital Certificate Authorities supported 1-5
  - encryption algorithms 1-4
  - key management 1-4
  - list of 1-4
  - management interfaces 1-4
  - monitoring 1-6
  - network addressing support 1-5
  - routing protocols 1-6
  - security management 1-5
  - split tunneling 1-7
  - system administration 1-6
  - tunneling protocols 1-4

fields, moving between 3-3

finishing Quick Configuration 3-22, 4-17

formats, data xi

H

hardware
- features 1-2
- installing 2-4

I

indicators, LED A-5

initialization and boot messages at startup 2-11

installation
- preparing for 2-1
- typical 1-8

installing
- in rack 2-4
- rubber feet 2-6
- the VPN Concentrator hardware 2-4

interfaces
- configuring 3-4, 4-2
- modifying 3-5

internal authentication server 3-12, 4-9
Internet Explorer, requirements 2-2
Invalid Login or Session Timeout error A-2, A-3
IP interfaces, configuring 3-4
IPSec Group, configuring 3-18, 4-14

J

JavaScript
  error A-3
  requirements 2-2

K

Kerberos/Active Directory authentication 3-16, 4-13
key management features 1-4

L

LED indicators
  100 (Ethernet) A-7
  Active Sessions A-6
  Activity (SEP-E) A-7
  Coll (Ethernet) A-7
  CPU Utilization A-6
  display at startup 2-11
  Ethernet Link Status A-6
  Expansion Modules Insertion Status A-6
  Expansion Modules Run Status A-6
  Fan Status A-6
  Link (Ethernet) A-7
  Power (SEP) A-7
  Power Supplies
    front panel A-6
  Status (SEP) A-7
  System A-6
  table A-5
  Throughput A-6
  Tx (Ethernet) A-7
  usage gauge A-6
licenses and copyrights B-1
Link LED (Ethernet) A-7
logging in to the VPN Concentrator Manager 3-1

M

management interfaces, features 1-4
memory, upgrading viii
mistakes, detecting and correcting 3-3
Model 3005, features 1-2
Model 3015, features 1-2
Model 3020, features 1-2
Model 3030, features 1-3
Model 3060, features 1-3
Model 3080, features 1-3
modifying an Ethernet interface configuration 3-5
monitor
  settings 2-3
monitoring
  features 1-6
mounting in rack 2-4
moving from field to field 3-3
MTU field 2-17

N

Netscape Navigator
  requirements 2-2
network addressing support features 1-5
network cables, connecting 2-9
No such interface supported error A-4
Not Allowed error A-4
Not Found error A-4
notices, regulatory agency B-10
NT Domain authentication server, configuring 3-14, 4-12

O

old browser (error) A-3
organization of manual vii
OSPF 3-9
Out of Range value (error) A-5

P

parameters needed for quick configuration 2-13
password
  admin, changing 4-17
  default login 2-15
  user database (CLI) 4-9
Passwords do not match (error) A-5
per-user address assignment 3-17, 4-7
physical site
  access to device 2-2
  cables and connectors 2-2
  cooling 2-1
  power 2-1
  preparing 2-1
physical specifications 1-8
power
  cable, 2-9
  requirements 2-1
  specifications 1-9
powering up 2-11
Power LED (SEP) A-7
Power Supplies LEDs A-6
preparing to install VPN Concentrator 2-1

Q

Quick Configuration
  beginning 2-12
  finishing 3-22, 4-17
  running only once 2-12, 3-1, 3-3, 4-1
  saving 3-22, 4-18
  starting
    from the console 2-15
    with Manager 3-3
  steps in 2-12
  testing 5-1
  using nondefault values 2-13
  using the VPN Concentrator Manager 3-1
  with Command Line Interface 4-1

R

rack mounting 2-4
RADIUS authentication 3-12, 4-11
reboot system
  saves log file A-1
regulatory agency notices B-10
related documentation viii
remote access, configuring 3-19, 3-20, 4-14, 4-16
removing a user 3-18, 4-10
Require Encryption option
  L2TP 4-6
  PPTP 3-9, 3-10, 4-5
requirements
  browser 2-2
  console 2-2
  Internet Explorer 2-2
  JavaScript 2-2
  Netscape Navigator 2-2
RIP 3-9
routing protocols features 1-6
rubber feet, installing 2-6
running configuration 3-3, 4-1

S

SAVELOG.TXT file A-1
Save Needed icon 3-3
saving the active configuration 2-17, 3-23, 4-18

screen
Address Assignment 3-10
Admin Password 3-21
Done 3-22
initial configuration 3-3
IP Interfaces 3-4
IPSec Group 3-18
Main 3-3
Protocols 3-9
System Info 3-8
User Database 3-17
WebVPN 3-19
WebVPN Portal 3-20
welcome 3-3
SDI authentication 3-15, 4-12
security management features 1-5
Session Timeout error A-2, A-3
size specifications 1-8
software authentication servers 1-5
software features 1-4
specifications
cabling distances 1-9
cooling 1-8
physical 1-8
power 1-9
size 1-8
standards compliance 1-9
split tunneling 1-7
standards compliance B-10
specifications 1-9
starting Quick Configuration 2-12
with Manager 3-3
startup
boot messages 2-11
initialization messages 2-11
static routes 3-9
Status LED
SEP A-7
steps in Quick Configuration 2-12
stopping the Command-Line Interface 4-18
system administration features 1-6
system information, configuring 3-8, 4-4
System LED A-6
system name, assigning 3-8, 4-4

T

terminal emulator
settings 2-11
starting 2-11
testing the VPN Concentrator 5-1
Throughput LED A-6
time
Daylight-Saving 2-16, 3-8
setting 2-15
zones, setting 2-15, 3-8
tools needed for installation 2-4
troubleshooting A-1
files created for A-1
tunneling protocols
configuring 3-9, 4-5
features 1-4
tunnels 1-7
Tx LED (Ethernet) A-7
typical installation 1-8
typographic conventions viii

U

unpacking 2-3
upgrading
bootcode viii
memory viii
usage gauge LEDs (table) A-6
user
adding 3-17, 4-9
deleting 3-18, 4-10

user administrator requirements 2-1
user database, configuring 4-9
using VPN Concentrator Manager functions 3-23

V

VPN Concentrator
  configuration settings for testing 5-1
  functions 1-7
  hardware features 1-2
  how it works 1-7
  installing hardware 2-4
  physical specifications 1-8
  picture of 1-1
  software features 1-4
  where it fits in your network 1-8
VPN Concentrator Manager
  errors A-2
  logging in 3-1
  logging out 3-23
  starting Quick Configuration with 3-3
  using for Quick Configuration 3-1
  using functions 3-23
  window 3-24

W

WebVPN 1-5, 2-12, 2-14
  configuring 3-19, 3-20, 4-14, 4-16
  setting up home page 2-14, 3-20, 4-16

Y

You are using an old browser or have disabled JavaScript (error) A-3